



Enhancing IT Contributions To Business Operations With IP Surveillance.

The Evolving Role Of IT In Business

As more business operations are evolved into IT applications, these operations are increasingly moving under the control and responsibility of IT management. The net effect has been that of boosting the IT department into a new position of responsibility and accountability. Businesses and other types of organizations are increasingly dependent upon IT not only to streamline internal operations, but also to sustain and improve business. To meet these objectives, it is critical that IT deliver operational excellence while demonstrating ongoing control, performance and ROI.

A new standard that has emerged for measuring and delivering IT practices is ITIL (The Information Technology Infrastructure Library), an industry best practice paradigm for IT service management. Having begun as a series of books, ITIL defines the organizational structure and skill requirements of an information technology organization and a set of standard operational management procedures and practices to allow the organization to manage an IT operation and associated infrastructure.

A key change to ITIL as it has been refined has been a new and increased emphasis in creating business value and ROI rather than just the competent execution of processes. IT is now as accountable as business units such as sales and marketing to add value, justify costs and enhance the profitability of the organization as a whole. This accountability will only increase over time as every investment made by an enterprise is closely scrutinized and evaluated for its

value to the business as a whole. IT organizations that fail to demonstrate control, performance and added value pose an unacceptable risk to business operations and prevent the business from realizing desired levels of return on their IT investments.

In addition to IT operations in line with the core activities of the business, IT responsibilities continue to grow for controlling internal business operations. IT must manage costs, guarantee security and integrity of business information, ensure availability and continuity of business operations, protect assets and reduce IT-related business risks. Increasing pressure to comply with regulations such as those introduced by the Sarbanes-Oxley Act, and the threat of civil and criminal penalties for infractions, heighten the pressure to deliver a greater level of control. As a result, it has become essential for IT to discover and develop strategies to accomplish these goals.

IP Surveillance – Beyond Physical Security

One tool that is finding increasing functionality to this end is IP surveillance. Having begun its long history as closed circuit television (CCTV) for physical premises security applications, CCTV originally provided a video stream to monitors that could be watched on-site by a guard, and that could be recorded for later use in identification of individuals or events. With the advent of digital technology and connectivity, cameras and other equipment have evolved and a wide range of products are now manufactured specifically for use on a network. As video surveillance system manufacturers and providers offer more products that run on an IP-based networked platform and users begin to implement these systems, the new IP surveillance is becoming an application which falls under the domain of the IT organization and for which the IT organization has responsibility as described by ITIL.

As IP surveillance has begun to be integrated on the primary IT backbone or a parallel IT network, a range of physical security and other applications for this

function have evolved. IP surveillance, as it is now termed, can be used in a number of different ways to add substantially to the overall contributions of the IT department, both internally and via profit-generating business operations.

Keeping pace with the migration from analog to IP for surveillance cameras and associated hardware have been advancements in surveillance software functionality. These have come both through interoperability with other applications such as access control, inventory management and Human Resources, and through the implementation of middleware to provide additional functionality like video analytics to track individuals, enable license plate recognition and identify risk situations.

IP Surveillance And Risk Management

Since Enron and other corporate scandals, in addition to the aftermath of hurricanes Katrina and Rita and the events of 9/11, risk management has grown in importance and is now a primary element of business operations planning. The feasibility of using IP surveillance as a tool to facilitate risk management is growing as new software to address this function reaches the market. With video analytics, it is no longer necessary for an individual to watch or review archived video in order to identify potential threats to safety or compliance. Advanced video analytics can be used to tag events or situations as diverse as a light out in a stairwell, a backpack left unattended in a vestibule, water left running in a bathroom, a flood in the basement or an individual slipping on ice outside the building. Wireless mesh networks and video mobility capabilities allow alerts and live streaming video to be delivered directly to a PC or handheld device including cell phones in any location, enabling quick response to help assure business continuity and safety.

Using IP Surveillance For Business Operations

A number of key internal business operations in addition to risk management can be addressed by IP surveillance. Using IP surveillance to demonstrate control,

performance and added value per the ITIL guidelines, and to create business value, will add to the ROI of implemented systems and to the value of the IT organization. A small representation of functional applications follows:

Asset Tracking

Archived video may be used to determine who has had possession of company assets at a given time.

Traffic Monitoring

For both automotive and personnel traffic, IP surveillance video can be a valuable research tool in evaluating usage patterns and any need for growth or change.

Inventory Control

For manufacturing facilities, retail establishments and warehouse operations, the ability of IP surveillance video to instantly track the physical location of inventory impacts throughput on many levels.

Identity Management

Video provides a backup verification that identification and access tools are only being used by the correct person.

Employee Productivity

While personnel and individuals in all situations have become accustomed to the presence of video cameras, the understanding that office or factory actions are being recorded can facilitate productivity. In the event of a drop in effective operations, video can provide needed information on personnel activities.

Liability Issues

Claims that are not supported by recorded data cannot hold up. Documenting events can help to protect businesses that could be vulnerable to litigation.

Process Monitoring

Finding the most cost and time-efficient processes by trial and error can itself be a difficult and time-consuming effort. IP surveillance can be used to help identify what is successful and unsuccessful and streamline processes to optimize effectiveness and quality.

Establishing Workflow/Consumer Buying Patterns

Whether used to track employee workflow practices or consumer shopping store aisles, IP surveillance video can provide management with information to help determine behavioral habits that impact the bottom line.

IT Operational Concerns for IP Surveillance

Integration of IP surveillance with the IT network raises the same operational issues that exist with the integration of any new system into the network. In order to maintain the standards that will enable them to meet ITIL mandates, the IT department must consider the following before making any determination of new products or solutions:

Network Utilization by Segment

If total network utilization (megabits of data per second) of a network segment exceeds the network's rated capacity, congestion and network degradation will result. IT needs to know the maximum network utilization of the IP surveillance system on any one network segment. It is also important to clearly identify maximum bandwidth utilization at any given moment as IP surveillance video is a bandwidth-intensive application that can quickly degrade network performance if implemented on an unprepared shared IT platform.

Aggregated Network Utilization

Regardless if the IP surveillance system is structured with centralized server based storage or recording is performed locally employing Network Video

Recorders (NVRs) or Digital Video Recorders (DVRs) with network capabilities, network traffic will be significantly affected by the number of cameras recorded, the rate at which they are recorded, and the number of cameras being recorded simultaneously. All these factors affect bandwidth utilization, making it essential to clearly identify IP surveillance system recording requirements so that IT personnel can recommend the most appropriate aggregate network utilization solution.

Quality of Service (QoS)

Network performance uninterrupted by events such as packet delays, jitters and drops is necessary for continuous transmission of bandwidth intensive content such as video. IP surveillance QoS is based on the highest amount of these events that the system can tolerate before it becomes too degraded to be considered viewable. IT uses these requirements to set up the system so that IP surveillance can function properly at the same time other applications are functioning properly.

Security

IP surveillance systems have the potential to compromise the security of the IT network if they are not set up properly. It is imperative that the IT group understand the IP surveillance security setup, particularly if encryption or VPN (Virtual Private Network) is used. IT may be called on to build the necessary IT security architecture for the IP surveillance system.

Location of Components

IT must be advised of the number and location of components (cameras, servers/ NVRs/DVRs/control points) in order for QoS to be implemented and the network sized appropriately.

Network Connections

IT must be advised whether IP surveillance components can connect to existing Ethernet ports or if new ports/switches (and of which type) will be needed.

Protocols

IT will use protocols to set up QoS for the IP surveillance network. Surveillance must advise IT which protocol they are using, which port in the IP packet it uses (if TCP) and what bandwidth requirements are.

Operations

It must be determined who will take responsibility for continuing operations of the networked surveillance system.

Conclusion

IT departments are no longer solely responsible for the operation and maintenance of computer systems, but are expected to perform in line with the ITIL paradigm. At the same time, a growing number of business operations are moving under the authority and responsibility of IT departments. While video surveillance was initially invented for physical security applications, its evolution to an IP-based platform has enabled a wide range of opportunities for the IT department to take a leading role in using the new IP surveillance as a business tool to improve operations and add value. Bringing this application under their authority, in concert with physical security operations experts, will enhance the position of the IT department within the enterprise.

XXX

For more information about Panasonic IP Surveillance solutions, please visit www.panasonic.com/i-pro.