Infinova®

The Integrator's Manufacturer

White Paper

Working with IT

A guide for Integrators and Installers on how to build an effective team with IT Managers.

Everyone involved with surveillance systems will be working with the IT Department more and more. For instance, over 75 percent of integrators report that they are spending more and more time with IT this year versus last year. In fact, 29 percent say they are spending significantly more time. If integrators are spending more time with IT, you can only imagine the impact IT has had on end-users. Why do we bring this up?

The ability to use network infrastructure is one of the major advantages of an IP-based surveillance system. Corporate networks typically provide adequate bandwidth and switching and routing versus coaxial cable. However, don't simply assume that running bandwidth intensive surveillance data over the IT network will be no problem. And, remember, especially if you are using high-resolution cameras, a lack of bandwidth will provide unsatisfactory images for the security department.

Here is the real problem. IT management doesn't always understand the actual impact of video on their network. Their most important concern is that video will overburden the network and, as a result, they panic.

This white paper is a guide for Integrators and Installers on how to work with IT Managers and get their buy-in and cooperation to build the best IP surveillance solutions for their customers.

Related White Papers from Infinova

Infinova has a series of white papers aimed at helping Integrators, CSOs and senior security management to make the technical and business decisions needed to manage security and surveillance installations. The previous five cover:

- Coexistence strategy at the heart of a cost-effective move from analog to digital security video.
- Selecting cameras – analog to IP-based as well as megapixel and high definition.
- Fiber optics enhances the operation and business bottom line of surveillance solutions.
- Storage options and ways to determine which are the best for the needs of the enterprise.
- How to conduct a security site survey leading to a risk and vulnerability matrix.

These previous white papers are available for download at www.infinova.com

Reality is a different story.
If the network is configured correctly, most corporate networks will have no problems handling video. The issue is the WAN when transmitting video between buildings. This is where it is very important to have the security and IT personnel singing from the same hymnal. Working together, they can design a better solution.

Nonetheless, security management seems divided. Some security executives welcome the involvement and ownership by IT of various parts of a video surveillance system while others see value in owning most of their gear. That's what you need to decide.

Whatever your decision, start off by making your IT department your partner. Don't get into a turf war with IT. It's their network and they will willingly share it if you include them from the beginning, get their inputs and advice, involve them in the approval processes and provide them with the necessary control. Sit down with your together with IT person to figure out how your video network will be implemented and who is going to own and be responsible for what parts of the project at installation and beyond.

For instance, show IT how placing servers close to the cameras for storage is a way to minimize transport of video over the WAN. Per their concerns, this is an extraordinarily important discussion to have with the IT department. By calculating the amount of bandwidth and storage that you will be needing, you can give them an estimate of the amount of data that your security cameras will send over the network.

Create a Security LAN
Fred Zagurski, CPP, CDT, principal of Fred Zagurski Consultants in Edmonds, Wash. recommends creating a separate Security LAN that will support intrusion alarms, access control, video surveillance and audio systems (intercom, P/A, mass notification, among others). This Security LAN should match existing LAN hardware, such as servers, monitors, UPS, core switches, edge switches, PoE injectors, routers and other equipment, and software (OS) as much as possible.

Some specifics include that the Security LAN shall use its own unique color cable to differentiate it from the corporate system. All cables, though, should be labeled using the in-house standards. It should also operate over a minimum of a 1 GB fiber backbone to assure it provides plenty of bandwidth.

Zagurski also suggests that the Uninterruptable Power Supply (UPS) be a smart unit that will sustain full operation for a designated period of time (approximately 15 minutes) before initiating shut-down. He recommends that the IT Department should have a one year warranty period to observe the Security LAN's reliability before deciding whether or not they want to connect the networks together via router(s). Lastly both networks should have the ability to shut-down for maintenance without affecting the other network.

What is your existing infrastructure?
Will this new video system bring pain to any existing infrastructure? Check with IT to determine how much bandwidth they can provide. They are likely to ask how much is needed. Make sure you don't shortchange yourself. Leave room for potential expansion in number of users / cameras.

IT will be worried that putting security video on the business network might hurt corporate network performance. Typically the IT Department's priority is to guarantee that email operation is uninterrupted 100 percent of the time. You should be concerned that the business system might cause you to lose recorded video. Should you share? Or, does it make sense to have two independent systems, thus, protecting both sides of the house, assuring that both can meet their mission objectives?

Perform a network assessment

Can you expect high qualities of service and expansion flexibilities from the network or will you need a sub-network? How is port capacity? These questions, and others, show the importance of working with IT.

As suggested by Zagurski, one solution that can work for both groups is using fiber optics. Since it is possible to send different frequencies of light over the same fiber, integrators can let the IT department know that they can transmit up to 32 videos over a single strand of fiber. Using a technique called wavelength division multiplexing or WDM, integrators can demonstrate how they can send four channels of video and bi-directional data over a single multi-mode strand of cable instead of the usual two strands. That means each strand of fiber can do more, saving the dark fiber. The IT department will appreciate how this procedure will free up their remaining fiber for other purposes.

IT also has standards

Take into account that IT also has standards and will require hardware testing before a storage device can hang from the network. Whatever you might be planning, don't forget to discuss firewalls with your IT contacts. DVRs need to be able to talk to their software through portals protected by firewalls that block out anything not recognized. Therefore, it's imperative to work with them up front on how to best accommodate their need for security, while providing access to the DVRs through those same portals.

Non-PC based DVRs (embedded) tend to recover better from power fluctuations than their PC based counterparts. They are not as susceptible to viruses, worms, Trojans or spyware. Not being computer-based, they are of little threat to corporate networks. Updates and patches require minimal IT involvement. They cost less, which the Procurement Department will like, and they are scaleable, which everyone will like as the system grows. Embedded DVRs feature a smaller footprint and there are large numbers of manufacturers and models from which to choose.

In addition, video storage needs are, in part, determined by the security video compression method. Newer compression technology, such as H.264, transmits only the parts of the scene that change from one frame to the next, helpful for maximum recording speed and longer storage capacity.

A Quick Glossary of Terms

How does that image created by a camera end up on a monitor? You'll find the IT department doesn't understand video-speak. Likewise security Integrators may not understand IT-speak. To help, let us define a network in IT-speak, discussing its various components:

- Network – A network is a group of computers connected together in a way that lets information be exchanged between the computers.
- Local Area Network (LAN) – A LAN is a network of computers that are in the same physical location, usually within a building or campus.
- Wide Area Network (WAN) – A WAN is used if the computers in the network are far apart, as in different cities.
- ISP – The Internet Service Provider (ISP) provides a direct connection between the LAN or WAN to the World Wide Web (Internet).
- IP Address – Internet protocol (IP) assigns a unique identifier to all computers and other devices connected to the Internet. Each device is assigned and can be identified by the unique address.

- Node – A node is anything connected to the network. Although a node is often a computer, it can also be a printer, a CD player…or an IP camera!
- Segment – A segment is any part of a network that is separated by a hub, switch, bridge or router from another part of the network.
- Hub – A hub is a connection point for devices in a network. It connects the segments. Think of a hub as an intersection where everyone has to stop their car (or packet of information). If more than one car reaches the intersection at the same time, they have to wait for their turn to proceed.
- Switch – A switch is like a cloverleaf intersection at the hub. Each car takes an entrance ramp to where they want to go without stopping or slowing down.
- Bridge – A bridge connects two LANs or two segments of the same LAN using the same protocol, such as Ethernet.
- Router – Routers forward data packets along networks. A router is connected to at least two networks, usually two LANs, WANs or a LAN and its ISP's network.
- Network Interface Card (NIC) – Every computer and most other devices, including IP cameras, are connected to the network through an NIC. Often, this is an Ethernet card. You'll find the slot on the back of your computer.
- MAC Address – The Media Access Control (MAC) is the physical address of any device on the network. It identifies the company that made the NIC as well as the serial number of the specific NIC.
- Quality of Service (QoS) – This is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For instance, if there is an emergency alert, that flow of video would take preference to others.

Glossary of CCTV terms
If you would like to provide your IT department with video terms and what they mean, simply go to this link: http://www.infinova.com/?cometo=diswhitepaper&whitepaperId=12.

Realizing the prospective growth of IP video, video management software companies are now creating video management software to help manage the capture and storage of video content. Likewise, video surveillance hardware manufacturers are working with them to assure that the transportation of IP images will yield clean, usable video. When migrating to IP video surveillance, you will want to assure that the video hardware provides an agnostic software interface so that the software wanted can be the software used.

By helping channel partners provide their customers with complete, affordable, best-in-class, large and small video surveillance solutions, Infinova helps integrators generate more business more profitably. Leveraging a manufacturing process certified to ISO 9001:2000 standards and over 250 engineers with a list of video industry firsts, Infinova channel partners provide their end-users with industry-acknowledged product reliability and technical leadership.

So that Infinova channel partners can create complete solutions, Infinova provides IP surveillance cameras and components, CCTV analog cameras, DVRs and components, camera accessories, monitors, power supplies and fiber optics communications devices. Infinova also has the technical ability and manufacturing flexibility to let integrators propose customized solutions. In addition, Infinova will partner with other manufacturers making other surveillance equipment and software to help its channel partners create turnkey solutions. Contrary to most other companies, Infinova will back-up their partners' products as well as its own to assure both the integrator and its customers that one call – to Infinova only – takes care of everything.

Infinova works diligently to assure its channel partners can provide cost-conscious solutions. With Infinova's hybrid systems, channel partners can propose systems that protect a customer's investment in its already-installed analog surveillance system but that also put them on a dynamic migration pathway to IP systems.

Infinova is lauded for its exceptional maintenance programs. A major highlight is the company's 24-hour advanced replacement policy in which a substitute product is shipped immediately upon notice of a problem.

With such customer focus, Infinova is often referred to as "the integrators' manufacturer."

Global Contact Information

Infinova®
The Integrator's Manufacturer

World Headquarters

Infinova
51 Stouts Lane
Monmouth Junction, NJ, 08852
United States
Phone: +1 732 355 9100
+1 888 685 2002 (toll-free)
Fax: +1 732 355 9101
E-mail: Sales@infinova.com

North America

Toll Free: +1 800 563 5564
Phone: +1 613 591 8181
Fax: +1 613 591 7337
E-mail: sales@marchnetworks.com
info@marchnetworks.com

Middle East & Africa

Infinova Middle East (Kuwait)
Phone: +965 2565-9818
VoIP: +1 7326473881
Fax: +965 2562-9491

Infinova Corporation (Dubai)
Phone: +971 04 399 5525
Fax: +971 04 399 5531
E-mail: Sales-ME@infinova.com

Europe

Phone: +39 0362 17935
Fax: +39 0362 1793590
E-mail: sales@marchnetworks.com
info@marchnetworks.com

Latin America

Phone: +52 55 5259 9511 / 7913
Alternate: +1 561 309 3308
Fax: +52 55 5257 0452
E-mail: sales@marchnetworks.com
info@marchnetworks.com

Hong Kong

Phone: +852 27956540
Fax: +852 27967740
E-mail: Sales-HK@infinova.com

India

Main: +91 020-412-14321
North: +91 989-912-1215
East: +91 900-700-4390
South: +91 968-6481834
West: +91 982-017-9808
E-mail: Sales-IND@infinova.com