ACCESS CONTROL & SECURITY SYSTEMS MAGAZINE

July, 2008

BUILDING A CASE FOR A MORE ROBUST NETWORK

By Paul C. Boucherle CPP, CSC

I have discovered what I believe to be a universal truth — every IT person wants a larger, faster, more scalable, and more robust network. Being a "recovering electrical engineer" who has worked on network-centric systems for the last eight years, I can understand this on a very visceral level. This one truth can be used to the advantage of those advocating convergence strategies. Building the business case for a more robust network requires understanding of the best ways to optimize a network from an investment and performance perspective, which include mapping security into the actual business value.

What exactly do we mean by "a more robust network?" Robust doesn't just mean a network with big bandwidth. It also means a system that is capable of coping with anticipated and unanticipated variations in its operating environment with minimal damage, alteration or loss of functionality. Robust also means dynamically flexible and adaptable in cost-effective ways, which will support Return on Security Investments (ROSI). Convergence of physical security systems onto a network, in order to ensure availability and reliability, requires additional bandwidth, routing of data for storage and segmentation from standard network maintenance functions.

Understanding the big picture can help to justify a robust network. New video technology allows for access to critical data in real-time by authorized department heads, thus helping to support faster and more accurate decision-making. Delivery of data to the right people at the right time certainly increases the ROSI potential for any company considering the investment. But first you must understand the company's business.

A common misconception about putting physical security applications on the network is the old argument about "putting all our security eggs in one basket." With modern network design, the network can be segmented in ways to satisfy even the most stringent performance and data security requirements. Make no mistake: this is a critical step that must carefully outline the user's requirements for availability, privacy, storage reliability and quality of data before proceeding with the network design.

Before a network can be redesigned for optimal performance, one must understand how, when and where various stakeholders will be using physical security system data to manage the business. A good rule of thumb is to begin the design criteria with the end in mind. In other words, what will network loading, storage and delivery needs be in a three- to five-year planning window? What departments will need to access data?

Consider these questions when evaluating building a more robust network:

Why might an end-user consider a more robust network?

Simply put, because there are long-term cost savings associated with installation and maintenance. The days of discretely wired low-voltage systems are rapidly coming to an end because a more cost-effective model — the network — is available.

Working backward from the desired end-state can provide a clear picture of what the network capabilities, nomenclature and attendant cost factors would look like. After the future system

migration potential has been projected and agreed to by the end-user, the network building blocks can be accurately estimated to support future migrations; i.e., cost-effective scalability.

What drawbacks to the investment might be encountered?

- ## Can more services be added, such as wireless access, point-of-sale connection, alarm features, etc.?

Price vs. Cost - Price is short-term and cost is long-term. The cost becomes relative to the business value delivered by the new network. When analyzing the implementation costs of discrete physical security and safety systems, it becomes apparent that cable installation can easily comprise 35 to 40 percent of the physical security system installation. Multiply this cost for each different physical security system that will now be network-centric installed over a three- to five-year period, and the cost savings of a robust network become the basis for ROSI.

- *Size* - They say bigger is better, and I can't argue that as it relates to building backbone networks. The cost of high-quality fiber cable has come down substantially while the cost to install conduit, coring and trenching continues to rise based on labor rates. It's a good idea to put more fiber cable in than you think you will need by a factor of three. You won't ever have to say you are sorry later.

- ## Will it accommodate facility expansion?

Existing Equipment - Using existing network equipment is a smart move for a lot of reasons, but you must first do your homework. IT "real estate" is precious in communication closets. Whenever a network rack has low port density and relatively new switch technology, there is an opportunity to leverage your current network investment. Racks and their support equipment (power supplies, UPS, cooling systems, backbone network patch panels, etc.) are expensive, take up space and generate heat. So anytime you can optimize existing equipment, it will lower the Total Cost of Ownership (TCO). The key element here: what does the switch technology look like, and does it have dual-plane network connectivity?

- *Training Expense* - Typically, IT departments have standards for hardware and software so they can minimize additional training costs through standardization of network hardware.

- ## What about long-term value?

Operating Overhead - Scalability allows for minimizing the number of people needed to administer the network effectively. Increasing the size and workload of a network can actually reduce the effective overhead costs of operation.

- *Maintenance* - Costs for maintenance will increase in direct proportion to the hardware installed to support the network.

- *Exposure* - Larger networks need to be carefully designed and implemented with all the necessary security procedures and protocols. This is especially true when wireless networks are incorporated into standard hardwire systems.

- *TCO* - As discrete physical security sub-systems such as video, access control, intercom, fire and intrusion detection use network protocol (TCP/IP) to deliver data, TCO factors decrease from both an implementation and service/maintenance cost. In addition, using existing IT resources to manage the network reduces outside contractor costs for normal preventative maintenance and even replacement of faulty hardware.

Can more services be added, such as wireless access, point-of-sale connection, alarm features, etc.?

The more work the network can facilitate, the lower the TCO for the network. Typically, back office support applications come to mind, but what about quality control, workplace safety, customer service, inventory control, manufacturing process monitoring, automated compliance and audit processes? When combined with physical security applications, these become a powerful argument for robust networks.

The evolution of wireless network technology has truly unlocked the door to delivering greater ROI for networks. The ability to extend network access to edge devices located beyond economically feasible locations improves security and data-gathering capabilities. As an example, look at how emergency communication stations have improved campus and parking lot security through integrated communications, two-way intercom and video verification.

Will it accommodate facility expansion?

Certainly if a company is growing its business, the need for additional real-time data is critical to that growth. As companies grow, lower expansion costs and better accessibility to business-critical data become a competitive advantage for any owner or senior management team.

If a company plans future expansion, the timing is perfect to step back and evaluate how a major construction project could leverage a needed upgrade of the network infrastructure. Any building expansion will require installation of the critical sub-systems designed to protect the building. The choice becomes… "Can we address this as we always have and use multiple suppliers, equipment and wiring to protect the building in a conventional manner?" or "Let's evaluate how a single network would handle a wide variety of infrastructure systems." It is likely the network-centric solution will be 15-20 percent more cost-effective to implement and 15-25 percent less expensive to maintain over the life of the system.

What about long-term value?

The key to long-term network value is in the backbone structure of a network. Fiber-optic cable does the job well, is flexible and can carry lots of bandwidth. Investing in a well-planned and redundant fiber network will stand the test of time. Newer technology, including wireless offerings such as Firetide and Fluidmesh networks, are extending our concept of what a Local Area Network (LAN) can do to support new network appliances in a cost-effective way.

It is clear: Building a robust network has significant advantages for many different departments including the IT department. An often overlooked strategy of gaining IT support is discussing any concerns about outsourcing. It is a significantly more difficult decision to outsource a network when physical security and safety systems reside on that network.

Paul C. Boucherle, CPP, CSC, is the principal of Matterhorn Consulting LLC. A security industry innovator of 31 years, Boucherle has experience as an IP video designer and consultant, system integrator, expert witness and IP video pioneer. He works with end-users, equipment manufacturers, system integrators and consultants. For more information go to matterhornconsulting.com or e-mail Paul@matterhorn.net.