

enterprising solutions

WITH ROBERT GROSSMAN

Upgrade or Replace: Questions Abound to Flesh Out Answers

One of the themes behind “Enterprising Solutions” is our focus on “real world” scenarios. Few of these hit closer to home for end users than the debate over whether or not to maintain, upgrade or replace aging electronic security systems. Should you maintain the status quo by performing maintenance and repairs? Upgrade a system (or portions thereof)? Or just chuck it all and replace it?

This is not simply a technical question. For many it encompasses all areas of a security operation and requires consideration of a number of factors. We’re presently going through this very equation with several clients and I thought I’d share some of our observations.

We’re not referring to building or adding on to a system. Instead, we’re going back to school this month and grading your systems in three ways: functionality (is everything working as required?), future (do they have the capaci-

ty to grow to accommodate near- to mid-term future needs?) and features (does your operation require specific features?). If your system gets one or more “F” grades in this report card, it may be time for a parent-teacher conference.

Functionality Is Key

Systems that are not functioning properly may be unreliable or of insufficient quality for the application. This includes:

- CCTV systems with poor image quality
- Access control systems that fail to permit access as needed (or grant it too freely)
- Alarm point monitoring that false alarms too often or doesn’t alarm when needed

An important question to ask is, “Can it be repaired cost effectively?”

Surprisingly, that question isn’t always as simple as it sounds. A system



Robert Grossman has spent more than 15 years in the industry and is president of R. Grossman and Associates (www.tech-answers.com),

a consulting group specializing in electronic security project integration, product strategy and evaluation. He can be reached at (609) 926-9264 or at rdgrossman@securitysales.com.

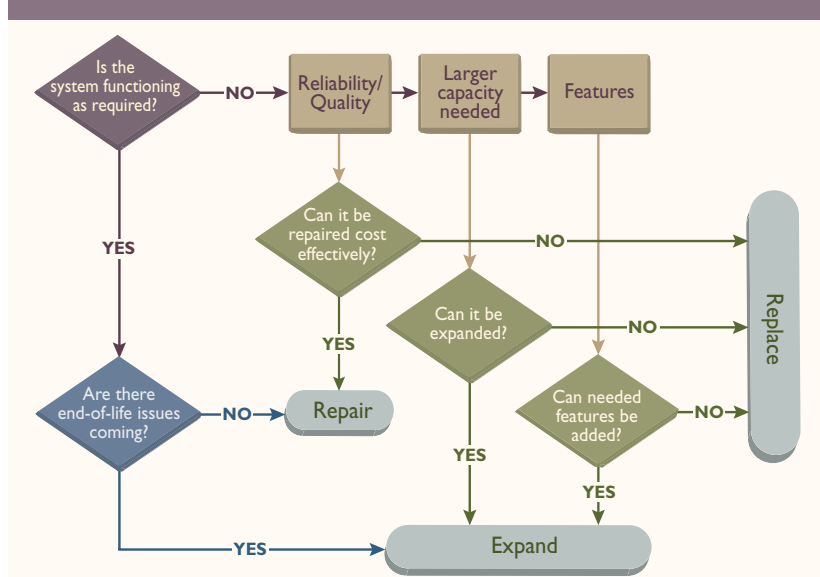
can be unreliable because of the application, hardware or installation. If it is either of the first two, you’re often better off replacing it. If the equipment isn’t right for your application, it will never be reliable. If the equipment isn’t up to the task, same answer. If the installation is at fault, you need to do some more investigating before making a decision.

You’re better off remedying some types of problems before you rip out a system and replace it with one that performs equally poorly. These can include: the wrong type of wire was pulled, the equipment was not terminated properly, power or thermal issues, or one of a host of installation-related gremlins. Very few careers can withstand these kinds of mistakes.

Another question that should be asked is whether or not the equipment is approaching the end of its serviceable life. We usually think of this being age-related (monitors, for example, have a finite operating life that is often exceeded), but there are two other reasons that come to mind. The first is whether the product still exists or is supported by the manufacturer.

I am working with one client who has an analog matrix switch that is about six years old. Ordinarily, this would not be an issue as matrix switching systems tend to be extremely reliable with 20-year operating lives. In this case, however, the switch manufacturer is no longer in existence, having long ago been acquired and shut down by the new parent company.

Chart Your Course



When considering a system upgrade or replacement, it is important to ask the right questions to obtain the right answers.

enterprising solutions

WITH ROBERT GROSSMAN

Since parts are no longer available, and the failure of this system would be catastrophic, they have no choice but to replace it.

The other end-of-life issue occurs when a technology is rendered obsolete and will shortly lack even basic market support. The best example of this is the multiplexer/VCR combination, which provides poor quality, low frame rate images and is subject to a host of problems that go unnoticed until there is a problem. The worst time to find out that the heads were worn on the VCRs, the tapes had not been changed or a power glitch had stopped the VCR is when there's an incident at your facility.

Newer technology has surpassed the realm of "nice to have" — the alternatives are so superior to tape — and has become a necessity. Other examples include DVRs and access control systems that use operating systems no longer supported by the manufacturer (Microsoft®, for example, has announced the end of the road for Windows™ 2000) or technologies that consume more space, power and cooling than their more modern counterparts (CRT monitors, for example).

If your facility is still hanging on to a type of technology like this, there had better be a plan in place to ensure replacement — along with a strongly written letter in a file to cover yourself when inevitable problems arise.

The Future May Hold the Answer

The second reason for performing the upgrade or replace analysis is to determine whether your systems can be expanded to the capacity you will need, and whether or not it will be cost effective to do so. Both sides of this question are equally important.

Often systems can be expanded, but if this pushes you up against the system maximums, the next round might not be possible. If that is the case, you may want to skip this expansion and replace the head-end with one that has more headroom. In other cases, expansion of older systems is not cost

effective. The older architecture may be expensive to incrementally scale, while a new system can offer greater capacity for less than expanding the old one. This is particularly true with older video matrix switches and some access control systems.

Look to preserve as much of the existing infrastructure as possible when

sion reported incident searches were shortened dramatically. "Searches that used to take days are now handled in real-time, while the person who is asking about the incident is still on the phone," remarked the surveillance director. "This has created a whole new direction for our department, allowing us to be far more proactive."

You're better off remedying some types of problems before you rip out a system and replace it with one that performs equally poorly.

making this decision. The cost of the head-end may not be prohibitive. However, any savings may be negated if all new cabling or other accessory devices are required. Manufacturers are moving more and more toward platform interoperability. You should be able to reuse a portion of your existing system or replace it in a later budget cycle.

Case in point: One CCTV system I am working with has called for a complete replacement. While we would like this to include everything, including eliminating oversized fixed camera housings and mounts in favor of sleek, miniaturized fixed domes, the image quality is remarkably good, particularly the black-and-white cameras. We've decided to defer that portion of the system replacement to another year, focusing instead on upgrading system control and adding digital recording.

Identifying Essential Features

While your system may be working well and have sufficient capability for expansion, it may be lacking features that are needed to effectively run your department. This can range from remote access to video files and system control, to fault tolerance for recorded images and data.

One gaming facility I worked with in an analog to digital recording conver-

Other facilities are looking to do things with their systems that current products simply don't allow. A mall is looking to allow limited access to its CCTV system during peak holiday seasons to measure the length of the Santa line or find the parking lot with the most available spaces. A company in a highly regulated environment is looking to improve fail-over provisions to ensure full compliance with all government regulations, including some that are only on the drawing board.

In these cases, expansion or repair is usually not an option; replacement of the system, or at least a portion of the system, is required to achieve the desired results.

One caution comes to mind: Security systems are very much "utility" type products. They were purchased to perform a specific task and, in many cases, they are still doing so reliably and effectively. If the needs haven't changed, and reliability is not an issue, don't rush in to upgrade software or firmware simply because the manufacturer now offers a newer version.

The old saying, "If it ain't broke, don't fix it" comes to mind, and the problem the manufacturer is solving may not apply in your application. They may have released a new version to solve one bug, but do you really want to be the one to discover the new bugs? ■