BOMA.org International

FEBRUARY 2005

THE MAGAZINE

Building knowledge and solutions to increase workplace performance.

Investing in Access Control and Security Systems: A Success Model

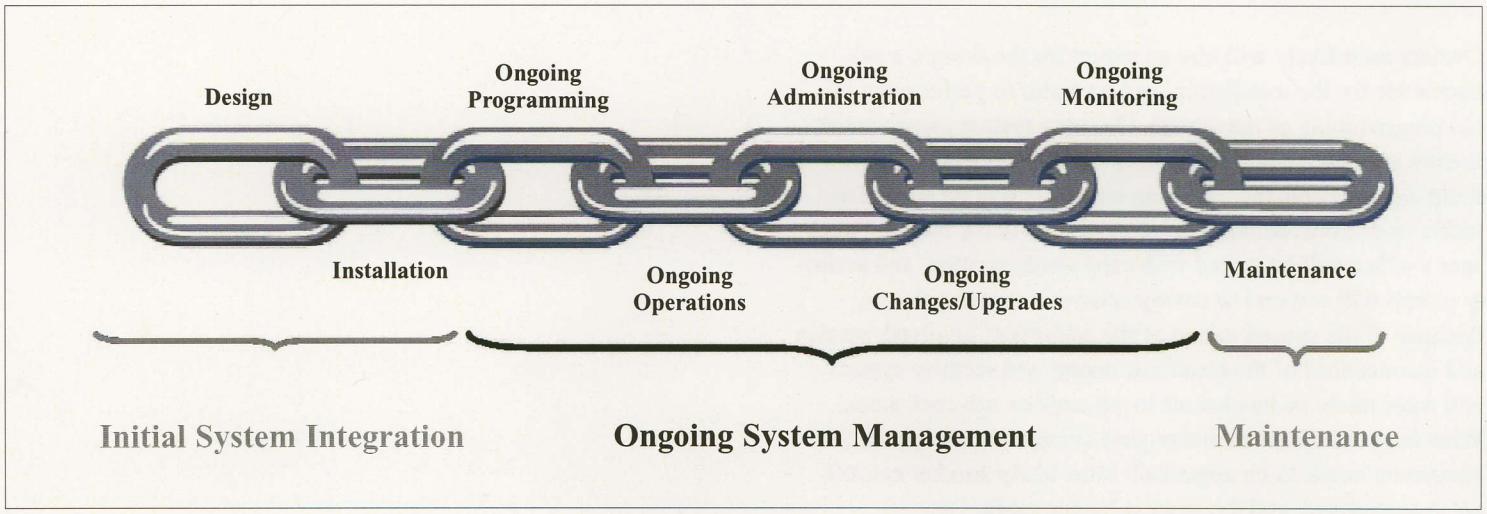
By Steven E. Rindner

To address tenant concerns and demands surrounding security during the past few years, many building owners hired experts to recommend access control and security systems, invested in the latest systems and components, and augmented their security staffs. Over time, however, tenant priorities evolved, security and administrative personnel turned over, and new operational challenges arose. Unfortunately, several years later, the buildings static security systems are inflexible and impractical for tenant use. In making the initial investment, owners and property managers relied solely upon great technology to deliver a total security solution, unaware they also needed to plan for ongoing system management (programming, operations, administration, changes/upgrades, and monitoring). The technology solution did not address the ongoing management of the system and lacked the necessary functionality, flexibility, and continuity to be effective over time. Confronted by the looming possibility they will be forced to abandon their investment, owners and property managers are experiencing a gap in their expectations between technology and functionality. This gap can be bridged by professional ongoing system management.

The Three Links in the Security Chain

Electronic access control and security may be compared to a chain that is only as strong as its weakest link. The segment of the security chain include initial system integration, ongoing system management, and maintenance. The initial system integration segment of the chain includes design and installation and consists of a customized needs assessment, threat analysis, and evaluation of security system options. The installation then delivers functionality through highly efficient off-the-shelf components tailored to fit the building s unique needs. However, purchasing only the first segment of the chain initial design and installation yields neither a comprehensive nor effective solution.

The middle segment of the security chain encompasses ongoing system management. That includes ongoing programming, operations, administration, changes/upgrades, and monitoring. This segment incorporates responsibilities such as administering access cards, ensuring building system performance, managing redundant



telephones, software, and manpower, coordinating multiple vendors, creating tailored response procedures, and specifying exception events. It also encompasses human resources responsibilities, such as covering for vacationing personnel, training operators, and establishing tenant protocols. To be effective, a system must be continuously and proactively monitored with protocols to address any situation or emergency that may arise. Conditions such as temperature, flood, smoke, and equipment failure must be monitored, as well as building perimeter and interior doors. Programming, backing-up the system, delivering preventive maintenance, and updating hardware/software round out the operational aspects of this vital, but often neglected middle segment of the security chain.

Preventive maintenance and service of hardware comprise the third and final segment of in the security chain. Warranties are imperative, but there is no substitute for having a knowledgeable professional on call.

All three segments of the security chain must be continuously provided to make the system function in a meaningful way. Building owners typically outsource the first and third segment in the security chain to professionals, but generally perform in-house the most critical segment —ongoing system management —leaving themselves vulnerable to the risk of the ever-widening gap between the technology they bought and the functionality they sought to achieve. Owners who have been successful bridging that gap have outsourced ongoing system management to professionals.

The Critical Middle Segment Ongoing System Management: Manage In-House or Outsource?

Owners have a choice regarding the ongoing operation and management of their system. They can assume the responsibility and liability by managing it in-house, or they can outsource the responsibility and liability of system management to professionals. Through basic evaluation, it is evident that staffing these ongoing functions in-house is not always practical or cost-effective.

Owners most likely will hire an expert for the design, a sub-contractor for the installation, and a vendor to perform the initial programming of the system. Ongoing system management is even more essential, but is often overlooked when a system is designed and deployed. Building engineers will be needed to tackle operations, administrative personnel in the building manager s office will be tasked with card administration, and security guards will respond to emergencies and monitor alarms. Because of the special nature of the equipment involved, service and maintenance of the electronic access and security system will most likely be handed off to yet another sub-contractor. What happens when tenants request changes to the system or equipment needs to be upgraded? Most likely another consultant is summoned, and the process begins again.

Outsourcing ongoing system management requires fewer in-house personnel and is significantly less expensive than creating a self-managed system. Over the life of a security system, owners experience dramatic savings in operating costs and achieve additional savings through the more efficient use of staff. Outsourcing also reduces the risk of potential legal liability. Hiring an expert to ensure the system is current and functional mitigates such risks.

The Benefits of Outsourcing Ongoing System Management

Owners typically rely on outside security professionals for the first and last segment of the system chain (initial system integration and maintenance). Owners should also consider outsourcing the critical middle segment — ongoing system management. Relying on security professionals for ongoing system management provides the experience, infrastructure, expertise and technical capabilities to secure a building. Experts do a better job because security is their core business, thus permitting a building owner s focus to shift from managing resources and issues to managing results. Also, it guarantees a reduction in costs and establishes a team of experts with the ability to adjust quickly to new developments and constantly changing technology, devices and threats. Professional ongoing system management eliminates the gap in expectations between technology and functionality. It ensures an owner receives the functionality, flexibility, and continuity of an effective, cost-efficient, long-term security solution.

Steven Rindner is Executive Vice President of Kastle Systems International, headquartered in Arlington, Va., and can be reached at: srindner@kastle.com or by calling (703) 528-8800.

"Reprinted from the February 2005 issue of BOMA.org Magazine, courtesy of the Building Owners and Managers Association (BOMA) International."