

October 15, 2003

Sophisticated security solutions

Zero tolerance for errors needed to protect and maximize technology investment

The technological revolution has touched every industry, bringing tremendous efficiency and productivity gains. The realm of security has likewise benefited from the boom. Complex command centers control global emergency response systems from a central location. Sophisticated access-control systems monitor times and locations of entries and exits, while biometric devices offer positive identification. Remote-controlled robots perform monotonous patrols, and motion-detection sensors linked to video cameras can instantly alert a security team to a potential intruder.

In many instances, implementation of technology reduces the number of security personnel required while increasing productivity. Even so, the human element of security remains a critical component of the overall program, often becoming even more important with the use of technology. Organizations that invest in cutting-edge systems must consider the quality of the human operators. Having the capability to detect an intruder in a remote location, for instance, becomes meaningless without the capacity to investigate and comprehend the situation immediately. On a more basic level, would senior management entrust a multimillion-dollar computer console to a minimum-wage employee?

Advances in technology can streamline security operations by limiting the number of uniformed employees required and by enhancing the capabilities of security officers. Over-reliance on systems and technology, however, can jeopardize facility security. After all, computers and machines are only as effective as the human beings who program and operate them.

Technology in the workplace

The old “night-watchman” concept of security no longer meets the demands of modern protection systems. Fierce competition in a global economy, combined with the heightened threat of terrorist attack, has prompted organizations to upgrade their security with technology, which can reduce headcount and improve performance.

Machines perform some functions more effectively than humans do. Some facilities use robots to patrol miles of corridors; unlike people, the robots do not fatigue or wane in alertness—a special danger during the midnight shift. At the same time, the robots themselves cannot investigate

anomalies they encounter; that task requires sound human judgement. The same holds true for the gains realized by using motion sensors and video cameras. While the devices can monitor a wider area more effectively, lack of alert, intelligent human responders nullifies their advantage.

Other advances significantly enhance the capabilities of uniformed security officers. For instance, some systems enable closed-circuit television (CCTV) operators to convert a recording of an incident to a digital video clip that can be e-mailed to the security director or other predetermined authority. Some handheld devices permit security officers to capture and transmit digital images to a control center for evaluation and direction, allowing security professionals to make real-time decisions based on reliable information. “Running the security machinery of a large-scale modern enterprise requires a familiarity with computer technology, which, unfortunately, a lot of the lower-paid and less-skilled guard forces do not bring,” said Richard Clarke, retired Special Adviser for cyberspace security within the National Security Council and the Designated Chairman of the President’s Critical Infrastructure Protection Board.

Even those systems unrelated to security require high-quality human protection. “People forget that their cyber and telecommunications systems are only as secure as the buildings and rooms that house them,” Clarke said. Security employees must restrict access to these sensitive areas and supervise the actions of cleared individuals, such as vendors and service workers. “All someone needs to do is have three minutes to look under mouse pads for a password and the entire network is compromised.”

Skilled employees: Value

The overriding concern in selecting the human element of the security program usually focuses on cost—specifically, on driving the cost as low as possible. The ongoing recession forces organizations in every industry to slash budgets wherever

(continued on next page)

Sophisticated security solutions

Zero tolerance for errors needed to protect and maximize technology investment

(continued from preceding page)

they can, and the invisible nature of the benefits of security often makes the security department one of the hardest-hit casualties in cost-cutting efforts: it's harder to quantify the savings of loss avoidance than to calculate the losses incurred by security breaches. Furthermore, many companies regard security services as an interchangeable commodity, similar to janitorial or catering services. This mindset deprives a firm of the skilled human resources needed to operate its equipment, providing a low return on the investment.

The growing complexity of the various systems used throughout a facility—including not only access control and intrusion detection, but also emergency response, inventory management and even office administration—requires high-caliber employees for effective implementation. As a result, companies need individuals who meet the following qualifications:

- Intelligent, possessing sound judgement;
- Educated and well-trained to ensure competent operation of the systems utilized;
- Experienced, with long tenure—otherwise, high turnover would render training efforts useless; and
- Interest and passion for the job to encourage peak performance.

By employing security officers with these traits, companies can maximize the return on their technology investment, utilizing the programs and equipment to the extent of their capabilities.

Success stories

Organizations that employ the same care in selecting human resources as they do in implementing technology realize tremendous savings and value.

One company in the Northwest faced the challenge of operating in a high-crime area. Using sophisticated cameras and communication equipment, the security team has significantly reduced

crime in the four-block area surrounding the facility. Security officers at the command center use cameras with pan, tilt and zoom features to monitor the immediate property, as well as out-buildings in the four-block radius, while tracking the progress of the patrolling officer. This employee keeps the command center apprised of his or her position and activity at all times. The center has the capability to record video clips, capture photographic images and monitor local police scanners—abilities that security officers have used to assist law enforcement in arresting individuals involved in graffiti, drug trafficking and destruction of public property.

In Silicon Valley, a 16-year veteran security officer acts as the security systems analyst for his client facility. His thorough understanding of the technology saves the customer thousands of dollars each year in service calls. When a vendor sold the client company software that was incompatible with the existing system, the officer studied the situation, explained why the system kept crashing and told the client how to remedy the problem.

A security officer in the Southwest manages the control center for an office complex, which integrates three systems: one that monitors all entrances, an access-control system and a burglary-reporting system. In addition to supervising the activity at the office complex, the officer serves as the central reporting contact for all remote locations. She has saved lives and prevented property damage through her ability to operate the equipment and dispatch medical and emergency responders in a timely manner. Her knowledge of the system also enables her to educate new employees who work at the control center.

A supervisor for a Midwest-based organization serves as the primary contact for maintaining all access-control equipment. Responsible for the card-access system and alarm monitoring throughout the company's multi-state region, this employee supervised the successful upgrade of all access cards and played a critical role in

converting the outdated communication system to one that utilized the latest telecommunication technology. Her assistance helped save the client millions of dollars, and she now helps with similar conversions at client locations nationwide.

A manufacturing facility in the Northeast increases productivity in several areas by using the technical skills of its security team. A senior supervisor works closely with the information technology (IT) department to help troubleshoot the client network; he also assists in developing network security solutions with the IT team and the local police department. Additionally, he studies technology trends and makes recommendations to help the customer keep abreast of new technologies. Another employee uses computer-assisted design (CAD) software to redesign emergency evacuation routes and signs at the facility, and she manages the system that generates employee payroll identification and computer network access identification. Other responsibilities include managing a database that tracks reservations for the numerous conference facilities on site, as well as operating multiple access-control systems.

Recipe for success

What traits do these security professionals share in common?

First, these individuals possess intelligence and judgement, which enables them not only to operate these highly technical systems, but also to respond in an efficient, appropriate manner. In the example in the Northwest, for instance, security officers must understand how to use the advanced features of the camera system to capture important details that will aid law enforcement in prosecuting perpetrators, while communicating with patrolling security officers to protect client property through immediate response. The employee at the control center for the office complex must monitor three systems simultaneously and quickly interpret their feedback to deploy the appropriate response teams. Failure on the part of these individuals would, at best, nullify the technological advan-

tage offered by these systems; at worst, incompetence could result in loss of life or property.

The employees described above all work at facilities that continuously challenge them to develop their skills and reward them for the added value they offer to the security program. The supervisor in the Northeast who monitors technology trends and the telecommunication conversion expert in the Midwest hone their skills to increase the efficiency of their respective client's security operations. This type of ongoing career development fosters loyalty and job satisfaction—two factors that encourage long-term tenure, which reduces costs associated with recruitment and initial training and allows companies to focus on improving the skills of an experienced security team. Without such nurturing and development, employees may become dissatisfied and seek other opportunities, forcing an organization to invest resources in cultivating basic competency in inexperienced workers.

A false sense of security

Even the most sophisticated security solutions are not foolproof, and virtually all require human intervention. Alarm systems, for example, are notorious for sending false alarms. Discerning between a false alarm and a genuine emergency requires an experienced individual with professional judgement and a thorough understanding of the system's features. Trusting a minimum-wage employee with the operation of complex systems can create a false sense of security and ultimately contribute to an organization's liability, a concept known as foreseeability—in which a company fails to take reasonable measures to prevent reasonably knowable risks.

Particularly in today's tight economy, obtaining budget approval for new technology requires concrete justification; the department requesting the system must demonstrate how the features of the equipment will meet a specific need. Approval of this capital outlay assumes proper implementation

(continued on next page)

Sophisticated security solutions

Zero tolerance for errors needed to protect and maximize technology investment

(continued from preceding page)

of all system functions. Team members throughout the organization trust that the men and women operating the system will do so competently and efficiently. If an emergency situation arises and improper use of technology hampers response efforts, the company could have liability. Management acknowledged the potential risks, evidenced by the investment in protective technology, but failed to protect its employees' and shareholders' interests by ensuring appropriate utilization of the systems. When the programs and systems in question affect emergency-response procedures, improper use could endanger the lives and safety of employees or visitors, further exposing the company to potential claims.

Another important factor to consider in selecting the individuals to operate security technology is the possible risk of entrusting those systems to people with malicious intent. For this reason, companies need to investigate the backgrounds of vendors, technicians and systems operators. Creating redundancies in the security process provides yet another level of protection. The potential use of "sleepers"—undercover terrorist agents who establish themselves in society before being called to action—presents a special danger, given the ongoing war against terrorism.

Selecting the right partner

Organizations that invest in advanced security systems must exercise the same diligence in selecting the people to operate those systems as they did in choosing the equipment. Companies need to identify, attract and retain high-caliber individuals to protect their investment.

Firms must ensure that their employees do not present a security threat, performing comprehensive background screenings on all applicants. Contractors and vendors must be held to similar standards in the selection of their employees.

Effective operation of sophisticated technology requires intelligent individuals with sound

judgement. Such employees expect commensurate compensation and benefits; furthermore, they desire the chance to develop their skills and advance their careers. Companies can maximize their investment through continuous education, teaching employees to perform a wide range of complex, technical duties. Combining other positions with security may reduce overall headcount, while bringing enhanced security awareness to non-traditional security roles.

Technology rarely provides a one-size-fits-all solution. Selecting the appropriate systems requires in-depth evaluation by experts, followed by periodic assessments to ensure that the systems continue to meet the organization's needs. A skilled work force will have the flexibility to adapt to any technology changes mandated by market trends and other factors.

Advances in technology have revolutionized virtually every industry in some way. The need to protect these sophisticated capital investments, coupled with the cut-throat competition of the global marketplace, continues to drive the market for leading-edge security solutions.

While many companies recognize the need for high-tech safeguards, an alarming number have ignored the equally urgent need to upgrade the skills of the people operating this equipment. This short-sighted approach poses several significant risks, including the potential for accidental damage to the equipment and possible liability for failing to implement all features of the systems in use. Organizations that invest in these technological advances must protect their investment by providing skilled operators who can supplement the technology with sound judgement. Their shareholders and the general public will demand nothing less.



The Lipman Report Editors