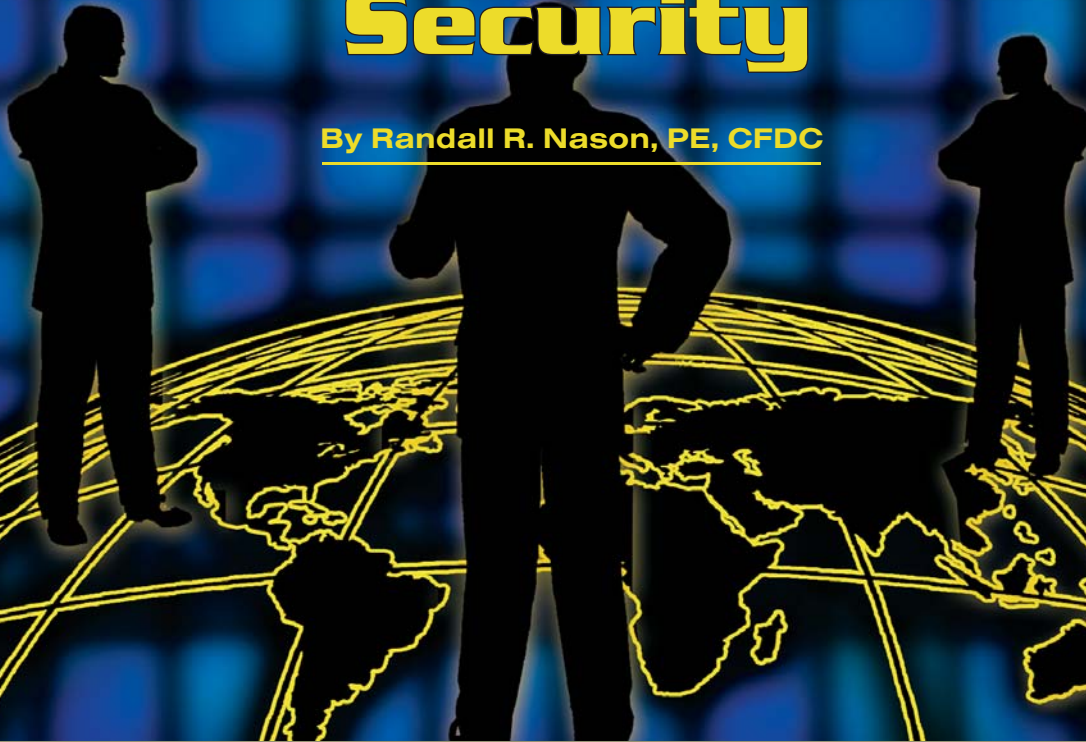


A Strategic Approach to Food Facility Security

By Randall R. Nason, PE, CFDC



**A leading
consultant
offers
a manageable
solution to a
complex
problem.**

The recent drive to secure the food chain requires a very thoughtful and strategic approach to ensure effective, consistent and cost-efficient implementation. This is especially true of organizations that have multiple, geographically dispersed facilities. Our experience in consulting to these types of organizations has resulted in a multi-step approach to achieve these goals.

FACILITY CATEGORIZATION. The first item on the program development list is to categorize your facilities. You don't protect a small five-person sales office in the same way as you protect your primary production facility. The key is to develop a process to segregate your facilities into categories of approximately equal risk and therefore similar security requirements. The problem then becomes manageable.

There are several ways to approach the process and a variety of factors to consider but the primary one to consider is the potential loss that could occur to the company as a result of a security incident at that facility. Whatever categorization formula is used must address this reality. Some of the factors that contribute to loss could include:

Population: How many people routinely work at a particular site? The greater the number of staff, the more the facility value increases due to the increased investment in office equipment and infrastructure as well as the simple value of human life.

Size of Facility: Simply speaking, the bigger the facility, the higher the value of

Multi-Facility Operations

the property. This is closely related to the population factor. Larger facilities have more people, more office equipment, larger computer networks, and in some cases, larger quantities of laboratories and test equipment.

Facility Function: A strong factor to consider is the facility function. The risk exposure of an organization is possibly less at a small distribution center than it is at the corporate product development center.

Value of Assets: One consistent measure of value in an organization is dollars: how much loss potential resides in a particular facility. This is a fairly easy factor to quantify in terms of hard assets as each site manager can usually closely estimate the value of the assets in his/her facility. The more difficult area to quantify is potential loss associated with damage to the brand.

Criticality to Corporate Livelihood: This is the definitive factor but one that cannot always be determined in isolation. This factor often comes into play when considering research and development facilities and data centers that may not be large or contain

to answer some very basic questions about application of security tools for a specific facility category. For example:

- What is an appropriate suite of security measures for each facility type? What level of security is really needed within each category? A four-person sales office may not need a fully implemented access control system like a 5,000-person corporate headquarters. In some cases, a simple intrusion detection system for after-hours monitoring may be sufficient.
- Does the criticality and risk of the facilities in this category justify the expense of CCTV monitoring? This decision not only involves the cost of CCTV camera installation but the digital recording and monitoring equipment and the staff time to manage and periodically monitor the system to ensure correct operation.
- How will system monitoring be handled? Will security be monitored on-site, by a contract third party, or by an off-site proprietary central station? Is the facility critical enough to justify a central monitoring station? If so, can additional economy be achieved by also monitoring additional sites? What kind of business case can be made for a corporately owned national monitoring center? Can the payback time be reduced by getting UL certification and also monitoring facility fire detection systems?

In some cases, the standards can be defined by a simple matrix showing the general types of systems to be installed at each facility category. In other cases, actual design details are prepared to define precisely how certain components are to be installed.

SYSTEM ARCHITECTURE. This part of the process has to do with defining what type of system will be installed as part of the long-term corporate goal for security. This part of the process involves answering questions such as:

- Will the security systems be isolated by site or will they be integrated as part of a larger enterprise system?
- Will the infrastructure backbone be provided by the corporate network or a dedicated security network?
- Will the system integrate with other corporate functions such as human resources?

Answers to these questions at an early stage will set the course for the long-term corporate security program.

PRE-APPROVED INTEGRATORS. When the project is ready to go out to bid for installation, it is usually time-efficient to have on hand a list of integrators that have been pre-qualified for the project based on past performance on previous projects. Establishing this list prior to the actual bid process shortens the bid review process by reducing the number of integrators to only those that have the demonstrated capabilities to successfully perform the project. This will significantly reduce the time required for the bid and review process.

It is important that a process be established whereby integrators can be pre-approved based purely on qualifications. This process increases the probability of having a best-in-class integrator on the project.



The definition of standards and processes must be viewed simply as a tool to increase efficiency. However, standards must never be allowed to drive the process to the extent that the real security needs are not met.

an overwhelming amount of hard assets; however, future revenues and the availability of corporate financial data rests on the continuous viability of these facilities.

One of the simplest approaches to facility categorization is by facility type. As a category, most office buildings for a particular organization will have a similar risk profile. This generalization also can be made for the other types of facilities such as product warehouses, processing facilities, and research and development centers. Each of these as a category could have category-specific protection templates that are applied by default. Site-specific differences often play a secondary role in the determination of the required security features. This approach works well for at least two reasons. First, the process is easy to apply and does not become encumbered with an overwhelming effort to collect site specific data. Second, for those organizations that do not exhibit large variations among facility types in the portfolio, individual site characteristics are not sufficiently variable to affect the final level of protection.

SECURITY STANDARDS. Now that the facility categories have been determined, the next step is to identify the appropriate security measures for each category. Development of standards forces you

DEVELOP STANDARD CONTRACTS. It goes without saying that nothing gets done without a contract. Therefore, it is essential that the same efficiency and functionality that was designed into the technical aspects of the program also be realized in the contracting procedures.

In most organizations, contracting is a highly specialized area of expertise accomplished by a separate line department with well-developed procedures implementing the checks and balances defined by corporate policy. Admit early that you will not change these procedures, but at the same time also commit to work efficiently within them.

Most of the time, a growing security program requires repetitive contracting actions as the same integrator does similar projects at separate facilities across the corporate portfolio. Therefore the key is to adapt the existing processes to quickly support repetitive issuance of project-specific task orders to one or more existing vendors.

INSTALLATION SPECIFICATIONS. Closely coupled with standardized contracting procedures are standardized installation specifications. Specifications textually define various requirements of the project that are not necessarily spatially dependent and therefore not easily represented on a drawing. Specifications will address such items as warranties, software functionality, testing procedures, material requirements, and security component characteristics. In many cases where the scope of the project is limited and the equipment to be installed is determined, the specification-like instructions can be placed on the drawings.

To the extent that the specifications are structured to deal with project specific items, some aspects of the specifications will change from project to project. However, most of the specifications should be constant, especially those sections that deal with equipment, means and methods, testing, and warranty requirements. Your expectations of the system integrator must be clearly defined in the project specifications. These expectations must be largely consistent from project to project so that the integrator can structure their organization to respond quickly and cost-effectively to the requirements of the contract.

Standardizing the contracts and the specifications should allow

you to proceed quickly with the real task at hand, and that is to reduce risk, reduce cost and increase customer satisfaction. Efficiency in the contracting process as well as the way projects are to be conducted is crucial in achieving these goals.

SYSTEM MAINTENANCE. It takes a focused effort to get a system properly designed, installed, tested and finally accepted. It takes a similar commitment to ensure the new system keeps running properly and efficiently. Maintenance needs to be considered in two areas: preventive and reactive. Preventive maintenance is just like an oil change; you know if you don't do it, something will break later. Hard drives need to be backed up, screws need to be tightened, and lenses need to be cleaned. Reactive maintenance is getting the recently discovered inoperable card reader on the main entrance door fixed fast. A key contributor to a good maintenance program is comprehensive testing. Written testing procedures along with a schedule can result in every component of a system being tested every six months or so.

The optimum maintenance program is always facility- and organization-specific. The best approach depends on the skill set of the security staff, the availability of in-house support, and the level of involvement desired by site management.

SUMMARY. The definition of standards and processes must be viewed simply as a tool to increase efficiency. However, standards must never be allowed to drive the process to the extent that the real security needs are not met. Standards must be viewed as guidelines that can be met with sufficient creativity of approach so as to satisfy the variety of real security issues that will be encountered.

The whole goal of the security program should be to adopt a posture of "This is how we do it," not "How should we do it this time?" This will eliminate a detailed decision process for each facility. In its place will be the application of developed guidelines through efficient facility surveys, facility appropriate design, and streamlined system procurement and installation. **AIB**

Randy Nason is a Corporate Vice President as well as Manager of the Security Consulting Group with C.H. Guernsey & Company.

FACTORS CONTRIBUTING TO A LOSS

- Population
- Size of Facility
- Facility Function
- Value of Assets
- Criticality to Corporate Livelihood

