Planning and implementing a security system requires more than updated technology. Taking a step back and analyzing both the physical and electronic components creates more effective and efficient protection.
INTRODUCTION
Prior to the Sept. 11 terrorist attacks on the World Trade Center and the Pentagon, the most significant threat to the United States’ nuclear power plant infrastructure was the former Soviet Union. At that time, governments believed that only foreign state actors or representatives posed a significant threat to national security. Security measures were based around this belief. For example, the Atomic Energy Commission (AEC) was created with the implicit understanding that a great security threat existed in the form of the “Communist enemy,” thereby putting the responsibility for nuclear power plant security solely into the hands of the U.S. government.

Since the end of the Cold War, the threat of attacks against the United States and other nuclear countries has evolved from identifiable state actors to adversaries with no state affiliation. Conflicts today are rarely fought on open battlefields — instead battles are fought daily against adversaries who are not always easily identified. The U.S. government has enacted laws and established governing bodies, such as the AEC’s successor, the Nuclear Regulatory Commission (NRC), to create minimum standards to protect infrastructure and mitigate these threats. But businesses and organizations have concluded that governments cannot be solely relied upon to provide protection against such threats. These entities must now become more self-reliant for the security and safety of critical assets and infrastructure.

Much like how the attackers have changed over the years, so have the tactics they use to carry out the attacks. Terrorist groups are constantly attempting to find new weaknesses to exploit. For each threat that is mitigated, another takes its place. This seemingly never-ending evolution of threats means that the methods and technologies used to protect our critical infrastructure must also evolve. Now more than ever it is imperative that nuclear power plants adopt a flexible security strategy that is adaptable to the ever-changing threat landscape.

THE DEFENSIVE STRATEGY
Unfortunately, there is no “one-size-fits-all” strategy that can be deployed at nuclear power generation plants. There are, however, minimum standards that must be met. Based on these standards, each plant must develop its own defensive strategy using comprehensive vulnerability, threat and risk analyses while considering the desired level of protection beyond the minimum standards, as well as other characteristics unique to the plant.

A defensive strategy is composed of all the security components of a facility. This includes policies and procedures, the security force, various components of electronic security systems and physical security systems, and the costs associated with the operation and maintenance of those systems. A defensive strategy will be affected by all other departments of a plant, from human resources and operations to the executives on the board. In order for programs to be effective, leadership must buy into the program, set the example and hold all personnel accountable. Doing so will assist others in recognizing the importance of the strategy and motivate them to take an active role in its success.

The backbone of any defensive strategy, however, is the security department. Each component within this department is affected by the operational capability of the other pieces within the security system. The security department relies on this technology to create a force multiplier, allowing it to more effectively and efficiently detect and respond to threats. In turn, the electronic and physical technologies in place rely on proper care and use to maintain operational capabilities to supplement the security department. Operation of the system relies
on the ability of the end users and management to properly utilize the systems in place and carefully research and implement components that can integrate and complement each other. This maximizes effectiveness, reduces costs and improves capabilities.

SECURITY FORCE
Just as the security department is the backbone of a plant’s defensive strategy, the security force is the backbone of the security department, providing the first and last line of defense. Even the most advanced technology in the world can’t completely mitigate threats without human interaction. A dedicated staff that can assess, respond and adapt to the changing battlefield is necessary to maximize the benefits of technology.

However, it is common practice throughout the energy industry to provide a solution by simply placing a security employee near the source of a problem. While this can be temporarily effective, it only benefits guard force providers, putting a financial strain on the nuclear energy industry by increasing operational costs.

Plants cannot sustain the use of a guard force as the sole solution to the protection of property and personnel in an industry where fluctuating fuel costs serve as the market motivator to work as lean as possible. Conversely, while there will always be a degree of human error or inability to prevent threats, technology alone cannot provide the critical thinking that is required to correctly assess and provide responses to security incidents.

ELECTRONIC AND PHYSICAL SECURITY TECHNOLOGY
Without the use of security technology, the profitable operation of a plant would not be possible because a large portion of the budget would be allocated to security personnel. However, too much or the wrong technology can put just as much financial strain on a plant as the costs associated with maintaining a security force.

Advances in technology have allowed security operations to become more cost-effective and efficient, optimizing the allocation of resources. Systems can be integrated to augment one another and make the process of deterrence, delay, detection, assessment and response initiation more seamless than ever. For example, intrusion detection sensors can be built into a barrier system, or cameras can be integrated with other sensors or alarms to provide timely remote assessment capabilities. This information can send alerts to monitoring personnel, automatically display a video feed of the area for assessment, or send real-time alerts and information to responding personnel to allow for faster and more accurate assessments and response.

With these technological capabilities, entities can minimize the amount of physical manpower required to maintain positive situational awareness, repurposing security personnel and possibly reducing operations and maintenance (O&M) costs. These technologies create force multipliers, allowing plants to carry out security-related tasks with more efficiency.
To reap the benefits that these advances in technology offer, careful and detailed planning must be undertaken to see that the various components are compatible with one another and have the necessary supporting infrastructure. Neglecting this aspect can render systems inoperable or plague a security organization with frequent false alarms or systems that do not function properly. Not only can this increase associated O&M expense by requiring frequent repairs or replacement, but also the costs of compensatory measures incurred during the outage of the system. It may also create an environment of complacency among security responders, who may develop a tendency to dismiss alerts as false alarms from faulty sensors.

The ability of the security force to utilize technology to its benefit must be included in enhancing a defense strategy. The system must be user-friendly for the security force to optimize the advantages of using technology and to demonstrate how security-related duties can be better performed. Technology should allow the security force to focus on other primary duties in lieu of carrying out tasks that could be augmented by technology. For example, vehicle screening technology may allow security personnel to more efficiently and effectively screen for possible prohibited items, minimizing errors in detection while decreasing time needed for screening.

OPERATIONS & MAINTENANCE COSTS

The Nuclear Promise initiative put forth by the Nuclear Energy Institute (NEI) has challenged nuclear entities to reduce costs by improving efficiencies and driving regulatory and market changes. Unfortunately, in a time when maximizing the effectiveness and capabilities of security programs is more important than ever, security is commonly one of the first items on the list of cost reductions. As security professionals, we are expected to do more with less — doing so still means making sure that the systems in place provide effective and efficient solutions.

To accomplish this, security components must be able to work cohesively. This requires that careful and detailed planning be performed to maximize the benefits and keep costs as low as possible. The operations and maintenance of these systems must also be considered during this planning process. System longevity and the ability to customize operational capabilities are important to achieving a return on investment.

ENHANCING A PHYSICAL PROTECTION SYSTEM

Staying ahead of newly evolving threats and tactics requires leadership to take an active and forward-thinking role to implement solutions. Systems that coincide with the operational environment and are within budget will provide the maximum benefits for both the security program and other areas of operation. Attaining these goals requires careful and detailed planning, as well as buy-in and involvement from various departments. This will allow plants to consider and plan for multiple aspects of any project, from security enhancements to construction.

ACTION BEFORE ANALYSIS

It has become common practice that when a plant identifies a need to upgrade or replace security systems, either electronic or physical, it will approach an equipment manufacturer to recommend solutions. This is common because a manufacturer may offer to complete an assessment at little to no cost to the client. Manufacturers agree to do this because, at the end of an assessment, their solution is usually to install their products. Unfortunately, the system or components that a manufacturer recommends may not be the best solution to meet a plant’s needs. It is possible that the solutions may not function appropriately with other components of a security system, resulting in issues and lost productivity due to the need for troubleshooting, repair or replacement.

Once recommendations are received from a manufacturer, a plant may approach a third party to oversee the design and implementation of the recommended systems. However, it is not unusual that the suggested components, be it a new fence line, vehicle barrier system or electronic security system, are not compatible without further modifications and engineering efforts, for which a plant may not have planned or budgeted. This can significantly increase costs, as well as place projects behind schedule, negatively affecting the outlook of the security program.
USING THE HOLISTIC APPROACH
When planning for the replacement or upgrade of security technology, it is important to analyze any components that may be affected to determine all possible consequences that may result from the upgrade. For example, if sensors along the protected area fence line are to be upgraded, it should be determined which sensors will be able to integrate seamlessly with the other components or if other hardware will need to be replaced or upgraded. Checking that the appropriate infrastructure is in place to integrate the new system(s) with existing systems will help with minimizing overall costs, project timelines and future operational issues that may arise. Other components that may not be directly related to security must also be considered. This includes the various engineering aspects that may need to be undertaken for the successful construction or installation of security components, including tangible details like structural, mechanical, electrical or civil engineering. It may also include non-tangible aspects, such as environmental concerns, including soil composition, grading or local environmental laws.

When the decision is made to undertake a security upgrade or replacement, assessments of other varying components of the defensive strategy should also be conducted. The depth of this assessment can vary depending on the project being undertaken; however, the overall goal with any project is to create or improve upon a system that can function uniformly with other components while also allowing for future modifications to be made without disrupting the system’s operational capability.

MAXIMIZING YOUR RESULTS
Partnering with a diverse workforce of engineers and security professionals to provide all the resources you need to complete a security or engineering project will garner success at your plant. Look for a firm that has demonstrated experience working at nuclear sites and across various other industries to bring lessons learned, best practices and other innovative solutions to the table.

Working with a firm that is not affiliated with any one supplier makes it easier to deliver a customized and detail-oriented solution that meets your exact needs.

Our firm uses a basic methodology which employs the following workflow, providing a structured methodology to:

- Gather all information that may be relevant to the project, including vulnerabilities, threats, risks and consequences
- Evaluate historical and potential risks associated with the site, as well as the present and future needs that will dictate selection of options
- Document findings and recommendations in an actionable report, including security design cost estimates for improvements
- Assess and present options for consideration to mitigate threats or enhance security capabilities
- Implement recommendations, including assistance with detailed design, procurement, installation and commissioning as approved and requested

Finding a partner that follows this basic format will help your nuclear plant employ the newest appropriate security technology while keeping O&M costs manageable.

BIOGRAPHY
KEVIN WHALEY is a physical security specialist in the security consulting group at Burns & McDonnell. With more than nine years of experience in physical security operations and management within the public, private and military sectors, Kevin brings first-hand knowledge in planning, designing and implementing security standard operating procedures. He has a thorough understanding of security technologies and how to effectively deploy these systems in a wide variety of environments, allowing him to specialize in conducting threat and vulnerability assessments and security management operations. He is a member of ASIS International and served in the U.S. military before joining Burns & McDonnell.