

Risks, Vulnerabilities & FACILITY MANAGEMENT

Maintaining safe facilities is more than just about checking people as they enter buildings; it now is also about protecting facilities from bombing and chemical, biological and radiological attacks.

By Michael Chipley and Jerry Kokos

Government agencies must revitalize their building security programs for new construction, or renovation and capital repair projects. Facility managers can integrate security practices into a facility management program creating a risk management program that mitigates building vulnerabilities. Combining security with facility management requires facility and security managers to identify the potential risks and hazards in building security, and develop long-term plans that ensure operations can continue throughout unforeseen emergencies.

Risk Management Program

Risk management is a systematic and analytical process that gauges the threats to assets, individuals, or functions, and identifies the actions needed to reduce the risk and mitigate the consequences of threats, according to the General Accounting Office. A risk management program is critical to mitigating building vulnerabilities. The goal of the risk management program, and of combining it with an existing facilities management program, is to evaluate systems in a manner that measures risk and the ability to recover, thus ensuring the continuity of the agency's mission and protecting employees, the physical infrastructure and other resources.

A sound risk management program begins with a threat and vulnerability assessment. It enables facility and security professionals to identify core organization functions, infrastructure, and physical assets, develop threat scenarios, determine vulnerabilities, assess and prioritize risk, establish optimal mitigations and countermeasures, and review security breaches. Implementing a valid and impartial vulnerability/physical security and condition assessment methodology is critical to the success of any risk management program. The assessment can give building owners and facility managers a clear picture of infrastructure and building vulnerabilities.

Identify Core Assets

Building and infrastructure condition assessments frequently are sparked by a number of factors, including legislation and executive directives, insurance industry trends,

financial accountability standards, and the very nature of potential threats themselves. A rational, consistent process for conducting security and condition assessments is essential to understanding what properties are in the

facility portfolio and pinpointing any potential weaknesses in security. Knowing which buildings are mission critical and determining which functions — administrative, data center, warehouse, mailroom, engineering, telecom switch, mechanical room, etc. — are "single point," non-redundant vulnerabilities will help direct the security planning measures. Further, it is equally important to identify suitable facilities where agencies can continue to perform critical tasks during the disaster recovery process. Armed with this data, both security and facility managers can measure possible risks against established safeguards, and then take critical steps to alleviate existing and potential vulnerabilities.

Once baseline condition information has been compiled, it can be used in conjunction with other assessment practices to detect threats and vulnerabilities to an organization's infrastructure. For example, a threat and vulnerability assessment helps agencies identify and analyze possible dangers, while other assessment processes evaluate assets based on the agency's operations, the group of people at risk, or the significance of a structure.

Assess and Prioritize Risks

Maintaining accurate, reliable information about infrastructure vulnerability and building security can be a challenge for building owners and property managers. But this is made easier if one follows facility management best practices. For example, the Capital Planning and Management Solutions (CPMS) approach. It combines threat and vul-



This image provides an example of blast analysis and effects radius.

nerability assessment methodology, Web-based technology and business strategies, and ensures credible, irrefutable data that can be used in the creation of security plans and when outlining building requirements. The data can lay the groundwork for collaboration and clear communication among government officials, agency leaders, facility professionals and security managers.

Maintaining facility data in a CPMS system that includes cost estimating capabilities also can aid the assessment and prioritizing of risks. Coordinating equipment purchases, including items such as intrusion detection systems and door alarms, and installation with capital investments that can range from electrical services to fencing, must be carefully planned to avoid out-of-cycle expenses, for example. With Web-based software, facility managers and security professionals can demonstrate the financial impacts of building repair and recovery in the wake of an emergency situation. The ability to perform “what-if” cost analyses gives agency leaders a clear sense of the financial investments and resources at hand.

It is critical to realize that each building varies in its importance in terms of a risk-management program. Every building has a primary function, such as providing health-care services or housing maintenance equipment. Prioritizing buildings according to the services and value they provide helps pinpoint which facility requires the greatest attention. Additionally, facility and security plans should incorporate “what-if” planning scenarios in case certain critical functions need to be transferred to other facilities in the event of an emergency.

Mitigate, Counter Security Flaws

When unforeseen emergencies arise, an effective mitigation or countermeasure will help uncover potential vulnerabilities proactively and strengthen an agency’s capability to continue operations. In the process of establishing mitigations or countermeasures, begin by examining the buildings that were earlier defined “critical.” Then identify existing vulnerabilities and weaknesses in those structures based on the threat and vulnerability/condition assessments and make recommendations to address those problems and potential hazards.

Additionally, it is important to develop a business continuity plan that ensures services can still be provided in the event that the security of each building has been breached.

Revising or acquiring new plans, policies, equipment and infrastructure also can help to identify and lead to mitigations and countermeasures. Infrastructure and equipment mitigations can include items such as gates, non-climbable fences and lighting that deters trespassers, and surveillance cameras running over the LAN and into a security operations center. Further, many of the principles of Crime Prevention Through Environmental Design can be combined with the Department of Defense Antiterrorism Standards for Buildings. (Page 35 — Ed.) An integrated site and landscape plan provides government agencies with standoff distance, access control and flow of people, as well as environmentally and architecturally appealing use of trees, shrubs and lighting to prevent access to critical areas.

Finally, establishing benchmarks to monitor the success and effectiveness of the integrated facility and risk management program is important. Have the vulnerabilities changed since the previous assessment? How so? Proven facility program measurements such as the Facility Condition Index and Facility Quality Index — percentages that quantify a building’s functional and physical inadequacies — also can be used to assess the success of risk management initiatives.

Conclusion

It is imperative that building owners, property managers and facility professionals address infrastructure security and building vulnerability. Likewise, both security and facility teams must be proficient with the technology and condition assessment methodology and understand their responsibilities, goals and objectives. Integrating risk management practices into a facility management program — and effective training of security and facility teams — decreases risk and increases success.

TMC

Michael Chipley is vice president of business development at UTD Inc., Manassas, Va.; mchipley@utdinc.com or (703) 393-0800.

Jerry Kokos is president and CEO of Vanderweil Facility Advisors, Boston; jkokos@vfa.com or (617) 451-5100.

Resources

Facility and security managers who wish to develop an integrated facility and emergency operations/disaster recovery plan will find these resources helpful:

- The Department of Commerce’s Critical Infrastructure Assurance Office’s Vulnerability Assessment framework; www.ciao.gov/resource/vulassessframework.pdf
- The U.S. Federal Emergency Management Agency’s “How-To Guide #7: Integrating Human-Caused Hazards Into Mitigation Planning;” www.fema.gov/fima/planning_toc6.shtm
- The Department of Justice’s Office for Domestic Preparedness, at www.ojp.gov:80/odp/welcome.html, offers help to state and local jurisdictions, including a grant program for the purchase of equipment, to respond to and mitigate the consequences of terrorist attacks; www.ojp.gov/terrorism/funding.htm
- The General Services Administration’s Public Building Standards; http://hydra.gsa.gov/pbs/pc/tc_files/tech_1.htm