

destroy property. When such measures are deemed necessary, law enforcement and other officials should work with the media to alert citizens to the security justifications for the inconveniences.

The main elements of infrastructure protection for major special events are as follows:

- Identify relevant infrastructure.
- Consider vulnerabilities.
- Coordinate and execute protective measures.
- Coordinate response plans.
- Consider cyber security issues.

This module will address each of those elements in turn. It will then separately consider issues related to cyber security.

Throughout the process of planning infrastructure protection, these are some key questions to ask:

- Have we conducted risk assessments on critical infrastructure and utilities that could have an impact on the special event?
- Have we collaborated with infrastructure and utility managers to develop adequate security plans?
- Have we coordinated with sanitation services for event security support?
- Have we considered protective measures for cyber systems in event of attack?

For major events, the infrastructure protection effort may be addressed by a dedicated planning team. For smaller events, the function might be part of an existing team's responsibilities.

II. Identify Relevant Critical Infrastructure

Exercise: Each student should take one minute to write a list of the critical infrastructure in his or her jurisdiction.

The instructor will write a sampling of them on a flip chart as students call out what they came up with. This gives students an idea of range of infrastructure types.

Over time, several different lists of critical infrastructure have been developed by various organizations. For example, the President's National Strategy for Homeland Security (2002)

Slide 4: Main elements of infrastructure protection

Slide 5: Key questions

Slide 6: Exercise

Slide 7: Infrastructure list

which infrastructure resources are both *critical* to the event and *vulnerable* to attack. Not every infrastructure resource meets both descriptions. For example, the local port may be vulnerable to attack, but the functioning of the port may have no particular bearing on the special event. Alternatively, highways leading to the event site may be essential for the success of the event, yet they may not be especially vulnerable. These are just hypothetical examples. Security planners should look at their particular situation and focus on those infrastructure elements that are both (1) essential to the event's success and (2) vulnerable to attack or disruption.

[Instructor: Remind students that they learned about conducting threat or risk assessments in Module 3.]

ASIS International (an association of private security practitioners) has published the *General Security Risk Assessment Guideline*, which offers both qualitative and quantitative techniques for assessing the risk and vulnerability levels at a given site. The guideline proposes the following steps:

- 1. Understand the organization and identify the people and assets at risk.** *Assets* include people, all types of property, core business, networks, and information. *People* include employees, tenants, guests, vendors, visitors, and others directly or indirectly connected or involved with an enterprise. *Property* includes tangible assets such as cash and other valuables and intangible assets such as intellectual property and causes of action. *Core business* includes the primary business or endeavor of an enterprise, including its reputation and goodwill. *Networks* include all systems, infrastructures, and equipment associated with data, telecommunications, and computer processing assets. *Information* includes various types of proprietary data.
- 2. Specify loss risk events/vulnerabilities.** Risks or threats are those incidents likely to occur at a site, either due to a history of such events or circumstances in the local environment. They also can be based on the intrinsic value of assets housed or present at a facility or event. A loss risk event can be determined through a vulnerability analysis. The vulnerability analysis should take into consideration anything that could be taken advantage of to carry out a threat. This process should highlight points of weakness and assist in the construction of a framework for subsequent

Slide 10: Risk assessment guideline from ASIS

analysis and countermeasures.

3. **Establish the probability of loss risk and frequency of events.** *Frequency of events* relates to the regularity of the loss event. For example, if the threat is the assault of patrons at a shopping mall, the frequency would be the number of times the event occurs each day that the mall is open. *Probability of loss risk* is a concept based upon considerations of such issues as prior incidents, trends, warnings, or threats, and such events occurring at the enterprise.
4. **Determine the impact of the events.** The financial, psychological, and related costs associated with the loss of tangible or intangible assets of an organization.
5. **Develop options to mitigate risks.** Identify options available to prevent or mitigate losses through physical, procedural, logical, or related security processes.
6. **Study the feasibility of implementation of options.** Practicality of implementing the options without substantially interfering with the operation or profitability of the enterprise.
7. **Perform a cost/benefit analysis.**

IV. Coordinate Protection Measures and Communicate with the Public

After determining which critical infrastructure elements are most vulnerable, it is time to consider how those infrastructure elements can best be protected. In some cases, the infrastructure is primarily on site and can be protected by the agency that is in charge of security for the event. For example, the vulnerability analysis might conclude that food prepared on site is vulnerable to tampering. In that case, the event security team can make plans to conduct background screening of food preparers, provide physical security to protect the food while it is unattended, and take similar protective measures.

By contrast, some infrastructure originates off site and cannot be protected well at the event site. In such cases, event security planners should coordinate their protective efforts with the main caretakers or originators of the infrastructure. For example, electricity is likely to be vital to the event. If power lines are buried and are not particularly vulnerable to attack in the vicinity of the event site, adversaries might decide to attack

Slide 11: Coordinate protection measures

transformers or other electrical equipment at some distance from the site. The equipment that needs to be protected may well be outside the reach of law enforcement. Event security planners should contact the energy provider and discuss security measures. The energy company may be able to increase security at its own sites during the special event.

Coordination in security planning is key. Just as terrorists are known for detonating secondary explosives as soon as emergency medical personnel arrive at the scene of the first explosion, they may also be able to increase the effectiveness of an attack against a special event by attacking not just the event site but also the local hospital, the routes to the hospital, or even electrical power at the hospital.

Protection of critical infrastructure is related to the security concept of rings of protection or layered protection. [Instructor: remind students that they learned about rings of protection in Module 7, Access Control and Credentialing.] Event security planners can extend protection beyond the event site itself to protect external resources or infrastructure that feed into the site.

In addition, law enforcement and government officials should work with the media to alert citizens to the security justifications for various inconvenient security measures. For example, at the 2004 Democratic National Convention, the Boston Police Department and the city removed public trash cans about a week before the start of the event. (Agencies cannot wait until the last minute to do everything; some things must be done earlier than others). Some members of the public were upset because when they cleaned up after their dogs while out on walks, there was nowhere to dispose of the bags. The removal of trash cans was inconvenient to them. Citizens then complained to the media. A proactive public outreach may help head off such complaints and encourage the public to be more cooperative with security measures.

V. Coordinate Response

The lead law enforcement agency in charge of security for a special event is unlikely to be able to respond alone—effectively—to attacks against most critical infrastructure. The technical demands of restoring electrical power, repairing broken water mains, or reestablishing telephone communications that have been cut are generally beyond the reach of anyone but a specialist in those areas.

**Slide 12:
Infrastructure
protection: an
element of layered
protection**

**Slide 13:
Communicate with
the public**

**Slide 14: Coordinate
response**

For that reason, law enforcement should establish contacts and coordinated response plans with the organizations responsible for critical infrastructure. Teamwork is likely to succeed best. For example, advance talks with the local electrical utility may lead to an action plan in which, in the event of a blackout at the site, law enforcement knows whom to call, makes that contact immediately, and makes officers available to escort and protect repair personnel.

VI. Cyber Security

One of the greatest potential threats to special event security may be a cyber attack. The National Infrastructure Advisory Council has noted that cyber vulnerability may lead to “an implicit or explicit failure of the confidentiality, integrity, or availability of an information system.” The fear is that a group could disrupt a major special event by infiltrating or hacking into on-site information systems that control communications, utilities (electricity, water, heating, cooling), or other essential information technology. Sometimes building controls actually reside in another city, where they might be even more vulnerable to attack by hackers.

The U.S. Secret Service has been leading the effort to develop cyber security for major special events. It has developed a partnership with the Carnegie Mellon University Software Engineering Institute’s CERT Coordination Center. The center is developing protocols to evaluate information technology security risks and implement protective measures. The U.S. Secret Service/CERT partnership can provide law enforcement agencies with cyber security guidance for special events.

Event security officials should develop plans in case an event is targeted. Efforts should involve mitigating the impact of the cyber attack and continuing services (backup/alternate plans for essential services). In order to obtain technical expertise to manage these cyber issues, local law enforcement may need to partner with universities or the private sector.

Another resource that may help law enforcement protect critical infrastructure during major special events is an organization known as InfraGard. Founded by the FBI, InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants,

**Slide 15: Address
cyber security**

dedicated to sharing information and intelligence to prevent hostile acts against the United States.

The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information and training that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes.

Question for class: Where would you go for help in planning cyber security for a major special event?

In sum, **protecting critical infrastructure and utilities** at major special events requires the following steps:

- Identify relevant infrastructure
- Consider vulnerabilities
- Coordinate and execute protective measures
- Coordinate response plans
- Arrange for cyber security.

VIII. Tabletop Exercise and Student Worksheets

A tabletop exercise was introduced in Module 1 and is used to demonstrate the need for pre-planning for major special events. The instructor should refer the class back to the tabletop exercise, anchoring teaching points to a common theme throughout the course.

Students should also work on the “Lessons to Learn” worksheet. The instructor should ask students to spend a few minutes completing this document, which will help them research and gain deeper knowledge about this particular topic.

Students should also work on the “Personal Action Plan” worksheet. This worksheet will help students develop specific steps, actions, or contacts and help them relate the material to events they are responsible for in their own jurisdictions.

Slide 16: Question for class

Slide 17: Conclusion

Slide 18: Tabletop exercise

Slide 19: Break