Countermeasures should be focused not only on security measures, but also on being balanced with the needs of the organization's daily business needs. Like all other business programs, compromises are necessary. What are the goals of countermeasures, given that compromises are necessary?

**COUNTERMEASURE OBJECTIVES, GOALS, AND STRATEGIES**

All security countermeasures have the broad goal of adjusting the behavior of potential threat actors so that they do not pose a threat to the organization.

There are three main goals for all security countermeasures:

1. Where possible, identify and deny access to potential threat actors.
2. Deny access to weapons, explosives, and dangerous chemicals to the facility (except for legitimate exceptions, which should be well controlled and monitored).
3. Make the environment suitable for appropriate behavior, unsuitable for inappropriate or criminal or terroristic behavior, and mitigate the actions of both hazards and threats.

Implementation objectives and strategies include:

- Control access to the target, denying access to possible threat actors.
- Where possible, deter threat actors from acting.
- Detect any threat action.
- Assess what has been detected.
- Delay the progress of any threat actor into or out of the facility.
- Respond to any active threat action.
- Gather evidence for prosecution, investigations, and training.
- Comply with the business culture of the organization.
- Minimize any impediment to normal business operations.
- Help to create an environment where people feel safe and secure and can focus on the purpose of the organization.
- Design programs to mitigate possible harm from hazards and threat actors.

Each aspect of the overall security program has the ability to support one of the three main goals. An incomplete example of how to map these is illustrated in Figure 15.1. You can use this as an example to help build your own list of countermeasures.

**ACCESS CONTROL**

*Goals:* Access control should be sufficient to facilitate access by authorized users and to deny access to unauthorized persons to all critical areas.

Unlike Fort Knox, most organizations rely on access by the public to their facilities. However, access should not be universal. All members of the public and all employees do not require full access to all areas of a facility. In the most humble shop, there is a public area and a storeroom/office. In complex facilities, access may be layered so that one needs progressively higher access authorization as one moves deeper into the facility.
**Countermeasure Goals and Strategies**

**Modes**

1. **Passive** — Screening of employees, contractors, and vendors
2. **Active** — Screening of entry by employees, contractors, vendors, and visitors

**Passive Strategies:**

- Develop an employee/contractor/vendor screening program
- Screen for criminal background, drug abuse (and financial responsibility where possible)
- Enforce it strictly

**Active Strategies:** Access control should be arranged in layers, typically including:

- Public areas
- Semipublic areas
- Controlled areas
- Restricted areas

- Public layers will be nearest the main public door, such as a public lobby, customer waiting area, or service desks.
- Semipublic areas are areas where the general public may not freely go, but where they may be escorted, such as to an interview or triage room or emergency department in a hospital.
- Controlled areas are for those individuals with authorization, such as non-public office floors, mechanical rooms, auto-mechanic work areas, airport tarmacs, and so forth.
- Restricted areas are those that require a high degree of vetting and where access is limited to a relatively small number of persons, such as research and development areas, the boardroom, main information technology server room, cash vaults, counting rooms, and so forth.

Access control can be achieved by technology or personnel means. There are two basic types of access control:

1. **General Access Control**
2. **Positive Access Control**

---

**FIGURE 15.1 Security Checkpoint**

- **Remove all metal objects before passing through metal detector**

- Three people standing in front of a metal detector, with a sign that reads, "Remove all metal objects before passing through metal detector."
General access control assumes that if one in a group has access to a space, anyone he or she is escorting is also permitted. This approach is commonly used in employee work spaces and the like, where an access card reader on a suite door controls access to the space. General access control should not be used where it is important to ensure that each person in a group has access privileges. This is because of the phenomena of an unauthorized person “tailgating” entry behind an authorized person as the door is opened. Although many organizations have tried to encourage employees to vet visitors who try to tailgate, none I know have fully succeeded.

Positive access control uses technology or guards to assure that each person is checked to be sure that they are authorized to enter the space. Examples of positive access control include card-reader–controlled revolving doors and turnstiles, theater or sports event ticket checkers, and airport boarding screening.

DETERRENCE

Goals

Deterrence is the ultimate goal. Deterrence achieves security without intervention against a threat actor. Deterrence builds its own momentum. The longer attacks are deterred, the less likely it is that an attack may take place.

Deterrence occurs when potential threat actors evaluate the risks and rewards of an attack and determine that the risk is not worth the reward.

- For terrorists, this could mean that an attack is not likely to succeed, that their attack would not capture the media’s attention, or that they could be perceived negatively by their own constituency.
- For economic criminals, it could mean that they may not be able to access the desired assets, or to leave with them, or the likelihood of capture after the heist would be high.
- For violent criminals, this could mean that the threat actor could not reach his target, could not succeed in the attack, or might not escape, or might be captured later.
- For subversives, this could mean that they might not succeed in subverting the normal operations of the organization.
- For petty criminals, this could mean that they might not be able to carry out their crime or would likely be captured in the act or later.

Strategies

Deterrence is achieved through making countermeasures visible enough that possible threat actors think twice about their crime. Deterrence countermeasures can include architectural hardness, access control measures, guards, obvious cameras, witnesses, alarms, and alarm signs. To be effective as a deterrent, countermeasures must be visible and must seem to create too much risk to carry out the attack. Ultimately, the entire baseline security program is about deterrence, and it creates the environment for all the other countermeasure functions (Figure 15.2).

There is no such thing as deterrent-specific countermeasures. All visible countermeasures can act as deterrents, but no countermeasures deter alone. Deterrence is a side
Countermeasure Goals and Strategies

Effect of the countermeasure’s other (primary) role. Countermeasures deter because the potential threat actor believes that the countermeasure creates risk to him. That risk is the result of the countermeasure serving its primary role of limiting access, detection, assessment, response, or evidence gathering.

DETECTION

Goals

Although at first the reader may be tempted to think that detection means catching the crook in the act, in fact every threat actor must carry out a plan in order to attack a facility. The basic steps in every threat action, whether it is terrorism or vandalism, include:

- Select an appropriate target for an attack.
- Surveil the target to determine the target’s vulnerabilities.
- Determine the best way to carry out the attack.
- Plan the attack (the approach, the attack, and the escape).
- Test the target to determine if the vulnerability assessment is correct.
- Execute the attack:
  - Enter
  - Establish and maintain control
  - Establish and maintain countersurveillance
  - Execute the objective
  - Escape

For petty crimes, all these steps may occur in one linear timeline. However, the more valuable the asset, the more important the attack is to the threat actor’s strategic goals, the more robust the countermeasures, the more time is required to carry out all these steps. Interviews with highly successful criminals indicate that the planning cycle
for some crimes can take months or even years. This gives the target many opportunities to detect the plan through the detection of surveillance and interception of planning communications.

**Strategies**

Strategies include surveillance detection and attack detection.

**Surveillance Detection**

Most people think of detection as occurring during an attack; however, detection can also occur during surveillance. Surveillance is required for virtually every attack in order to:

- Select the target.
- Surveil target vulnerabilities.
- Determine the best way to carry out the attack.
- Test the target to determine if the vulnerability assessment is correct.

Additionally, the longer a criminal spends time with eyes on the target, the more interaction he may have with individuals working in the target space. Each interaction gives the target opportunity to recognize surveillance, attack planning or testing, and interrupt the attack before it occurs.

A good countersurveillance program is highly useful to all organizations where asset values are high, and especially where there is a possibility of violence occurring in the carrying out of a crime. For terrorism, a good countersurveillance program is an absolutely essential component of any workable terrorism countermeasures program.

A good countersurveillance program includes:

- Ample use of video surveillance in exterior and public spaces
- Trained and alert security officers
- Trained and alert console officers
- Loitering detection software on the video system

**Attack Detection**

Once an attack of any kind is under way, whether it is terrorism, economic crime, violent crime, subversive action, or a petty crime, it is important, where possible, to be able to detect the crime under way.

Detection countermeasures may include:

- Intrusion detection system on property and building perimeters
- Intrusion detection system applied to critical passageways and internal spaces
- Duress alarms at critical counters and desks
- Hold-up alarms

Intrusion detection systems on property and building perimeters may include fence detection systems, microwave and infrared beams, seismic detectors, pneumatic line detectors, video fence-line detection systems, glass break detectors, and door position switches.

Internal space detection systems may include door position switches, area motion detectors, and video motion detectors.
Duress alarms may include hidden finger switches, foot switches, and so forth.
Hold-up alarms may include duress alarms and bill traps (last bill removed in a cash
drawer triggers a silent alarm).

Alarms may be either silent or audible. It is best to use an audible alarm if the prop-
erty is vacant, such as at nighttime, and the audible alarm could act as a deterrent, fright-
ening the intruder away. Silent alarms are best where an audible alarm could be false or
nuisance and where on-site security staff can respond quickly and where such response
would not possibly escalate the crime to violence.

ASSESSMENT

Goals

When an attack is detected, it is then necessary to assess the threat for the following reasons:

- Is the detection real, false, or a nuisance detection?
- If the detection is real, what are the level and nature of the threat actors?
- What is their goal?
- What weapons are they carrying?
- What are their tactics?
- Does this appear to be unfolding as a property or violent crime or a property
  crime with potential for violence?
- Are they employing countersurveillance methods?
- How are they dressed? How can law enforcement recognize the threat actors
  from ordinary employees or customers?
- What is their apparent exit strategy?
- Is the detection real, false, or a nuisance detection? Many alarms are either false
  or nuisance alarms. Before responding to any alarm, it is useful to investigate
  and assess to see if the alarm is real. This can often be done by using a second
  alarm device as a confirmation, or using a second technology to confirm. For
  example, on perimeter alarms where nuisance alarms are common, it is useful to
  have two types of alarm detection technologies, each having different nuisance
  modes, and both working together. For example, the use of infrared beams and
  fence line detection, where infrared is subject to nuisance alarms from blowing
  newspapers or animals, and the fence-line detection is subject to nuisance alarms
  from nearby trains. If only one alerts, it could be a nuisance alarm, but when
  both do, it is confirmed. Video cameras can also be used to confirm the alarm
  when the presence of an intruder can be seen on camera.
- If the detection is real, what are the level and nature of the threat actors? Once
  confirmed, it is important to know the nature of the threat actors. How many
  threat actors are there? Does their intrusion seem organized or chaotic? Is there
  an obvious leader? Is the group cohesive and professional, or are they displaying
  anxiety and fear?
- What is their goal? Are they carrying a sign protesting the activities of the orga-
nization, or are they carrying automatic weapons? How many threat actors are
there? Can their intentions be determined by their actions?
- What weapons are they carrying? If the threat actors are carrying weapons, what
  type are they? Are they knives, handguns, automatic weapons, rocket-propelled
grenades (RPGs), or mortars? Does the use of the weapons indicate a high degree of training, or do they seem amateurish?

- **What are their tactics?** The tactics of an individual or group speak to their capabilities and training and preparation to use force or to counter a security presence. Tactics may indicate that it is appropriate to confront or to stand off.

- **Could their intentions include violence?** Based upon observations such as their interactions with employees and customers, it may be possible to determine their willingness to use violence as a means to control the crime scene or to gain access to specific assets. The willingness to use violence may be important to help dictate your response.

- **Are they employing countersurveillance methods?** The presence of obvious countersurveillance such as a person waiting in a car nearby but not at the door indicates a high level of preparation and planning. This indicates that contingency planning may also be in place to deal with approaching law enforcement or the arrival of external security team members. The presence of countersurveillance will dictate different response strategies.

- **How are they dressed? How can law enforcement recognize the threat actors from ordinary employees or customers?** Whether the response will be by law enforcement or by internal security, it is important for them to know who are the threat actors and who are the victims. Otherwise, all persons will be treated as threat actors. This is especially true where the threat actors are using violence to control the crime scene.

- **What is their apparent exit strategy?** Often overlooked, it is important to determine the probable exit strategies, where possible. These may include:
  - A waiting car, perhaps with a getaway driver (look for a getaway car at all exits)
  - Waiting motorcycles or bicycles
  - The use of weapons to exit the premises
  - The taking of hostages
  - The staging of stolen goods (such as dumping jewelry into a dumpster for later retrieval)

  This knowledge can help to cut off the criminals or allow for the interception of the criminals or their stolen goods.

**Strategies**

Effective assessment countermeasures include video and voice communications systems. Video cameras should be placed at all facility perimeter areas, facility approaches, and facility entries in order to get a positive identification of any threat actors who enter the facility and to determine what external support they have in terms of lookouts and getaways.

It is very useful to have a video camera viewing every reasonable area where a threat action could occur, including all entry control locations. This allows both detection and assessment of crimes in progress. It is also very useful to have a two-way voice station (intercom station or station without call button) near the camera wherever a threat action could occur. This allows interruption of the threat action by a remote console operator, and for many crimes, this is enough to end the crime.
RESPONSE (INCLUDING DELAY)

Goals

Once a threat action is detected, a response is possible. Responses to threat actions could include:

- Take no direct action to counter the threat actors, instead try to minimize any potential harm to innocent people.
- Gather evidence for an investigation and for a postevent analysis resulting in scenario planning and training later.
- Call others (such as the police) for help.
- Intervene directly against the attack to stop it and capture the threat actors.

Before any response is undertaken, it is necessary to formulate an appropriate response. I propose that the best time to do this is before any attack, when heads are clear and planning time is leisurely. It may be necessary to adjust the plan if an actual attack takes place, but at least there will be a response plan in place.

For example, before September 11, 2001, it was the policy of airlines to cooperate with airplane hijackers and let negotiators arrange for freedom of the hostages once back on the ground. This strategy included allowing hijackers access to the cockpit to avoid casualties on the plane. However, when United Airlines Flight 93 passengers used their cell phones to call loved ones after the plane was hijacked, the passengers learned that another plane had crashed into the World Trade Center, the passengers changed the strategy from one of cooperation to one of counterforce. Although this strategy did not save their own lives, it did save many lives in the ultimate target, in Washington, D.C., and, as such, was certainly an act of heroism.

Strategies

Responses may also include delaying the threat actors, denying them access to the target asset, voice communications for negotiations, and ultimately force on force.

As a design consultant, I am a big believer in using technology to counter threat actors instead of placing lives at risk. The use of reactive electronic automated protection systems (REAPS technologies) may include two-way voice communications, delaying technologies, disruptive technologies, and active force technology for direct use against threat actors. See Chapter 16 for more on REAPS technologies. Also, REAPs technologies are covered in great detail in my book Integrated Security Systems Design.

Intercoms are the forgotten technology of security. Security intercom systems, along with ample use of security video systems, allow for immediate assessment of threat actions without dispatching a guard, which could escalate the crime to violence. One of the most effective tools against convenience store crimes has proven to be a two-way voice

communication system that allows console officers in a remote security command center to speak directly to store robbers, alerting them that they are not only being recorded by video cameras, but that their identification is solid and that police have been called and are on the way, and that any escalation to violence will result in more severe charges by law enforcement. This has proven to be effective to get robbers to stop the robbery and leave the premises immediately without further harm to the store employees or customers and in many cases also without completing the robbery.

It is very useful to have a two-way voice station (intercom station or station without call button) near the camera wherever a threat action could occur. This allows interruption of the threat action by a remote console operator, and for many crimes, this is enough to end the crime.

EVIDENCE GATHERING

Goals

The goals of evidence include providing resources for investigations, strategy development, and training. Figure 15.3 presents information on evidence gathering.

Evidence sources may include:

- Video footage
- Audio recordings
- Fingerprints
- Crime scene forensics
- Computer forensics
- Witness statements

Strategies

The security program should be designed to gather evidence from its outset, and personnel should be trained to protect physical evidence.

Camera placement should be useful to identify threat actors as they approach and enter the facility and at the most likely locations where crimes may occur. This requires, during the risk analysis, careful consideration of the types of threat scenarios that are most likely and the locations where such scenarios might occur. All these should be noted in the report.

Audio should be recorded on all outgoing calls to emergency responder phone numbers (911 in the United States and 112 in other countries) and on all active security intercom stations.

Security officers should be trained to secure a crime scene immediately after a crime until law enforcement arrives. Security barrier marker tape (“Crime Scene — Do Not Cross”) should be kept in stock for this use.

Any computers that could have been involved in a crime should be unplugged from the network but left powered on, secured, and sealed for the arrival of a law enforcement or internal computer forensics team.
COMPLY WITH THE BUSINESS CULTURE OF THE ORGANIZATION

Goal

Every organization has its own unique business culture. It may be formal or relaxed, top-down or lateral, or open for free movement of the public or imposing restricted movements. The security program should be configured to comply with the business culture of the organization. All security measures have some consequence both to normal business operations and to the business culture. Both should be minimized as much as possible.

I have been consulted on many projects to correct failed security programs that, upon review, were basically sound in principle, but which did not take the organization’s business culture into account and thus were not accepted by the users. The users are stakeholders in the system. If their point of view and expectations of convenience and perceived intrusion are not taken into account, the security provisions will not be accepted. This is the most important nontechnical element that addresses directly the success or failure of the system.
People will naturally take the path of least resistance. And, if after many years of moving freely, they are suddenly confronted by a queue or a barrier, they will attempt to circumvent it because they are used to being able to move freely through a portal without impediment. If there is a sneak-path, they will use it. If there is a guard, they will argue with him or her. There will be complaints, and pressure will be applied to the security manager to change the procedures or technology. It is important to take traffic flow, throughput, and people’s perceptions of how they are being treated by management into account.

Strategies

In the countermeasure planning phase, it is important to understand the organization’s business culture as much as possible. This is perhaps the most difficult task that a security practitioner has to do. Business cultures are rarely well documented. Culture by definition is that body of knowledge that is common and allows a common communication based upon shared assumptions of those working together.

For example, in one high-security project, the entire campus could be easily secured by moving all visitor parking to an adjacent parking lot and having all visitors clear through a single visitor center. However, the business culture of that organization required that all visitors be granted access to parking on the campus, thus allowing visitors past the visitor center. Security took second place to business culture.

It should be assumed that the security program should impede as little as possible into the movements of people, and the security program should ensure that everyone is treated with consideration, kindness, and respect.

MINIMIZE IMPEDIMENTS TO NORMAL BUSINESS OPERATIONS

Goals

As with business culture, all security measures have some consequence to normal business operations. The security program should impede as little as possible into the normal business operations.

Strategies

The key impediment to business operations is almost always in the area of access control. A key strategy of controlling access without creating the sense of an impediment is to rely more on technology than on people for security access control.

It takes more time to clear a staffed checkpoint than to clear through a card reader. And people tend to see technological delays as “part of the environment.” However, when the delay is associated with a security guard, they tend to personalize the screening action. (People sometimes presuppose a bias against the person by the screener and infer an intent on the part of the security officer to delay the person.) No such intent can be imposed on a card reader, as technology has no capacity to develop intent or biases or to distinguish any one person from another.
This strategy has other benefits as well. Because technology does not distinguish people, it treats everyone fairly and cannot be compromised by threat, intimidation, or enticement. All security officers dealing with the public should be trained to be gracious under fire and not to personalize any verbal abuse.

In areas where people are carrying bags or totes, provisions should be made to use as few hand actions as possible. In such cases, the use of photo IDs as an access vetting measure can help speed people along.

SAFE AND SECURE ENVIRONMENTS

Goals

Help to create an environment where people feel safe and secure and can focus on the purpose of the organization.

Strategies

The use of crime prevention through environmental design (CPTED) principles helps to create a safe and secure environment and conveys a feeling of safety and security to all.

Good lighting, gracious guards, well-maintained facilities and security equipment, good way-finding signage, security awareness inserts in the company newsletter — all these things contribute to a feeling of well-being on the part of users.

DESIGN PROGRAMS TO MITIGATE POSSIBLE HARM FROM HAZARDS AND THREAT ACTORS

The security program should include elements to deal with unwanted exceptions, such as:

- Intruders and Offenders
- Disruptive People
- Medical Emergencies
- Natural Disasters
- Civil Disorder and Riot
- Loss of Business Continuity
- Chemical, Biological, Radiological Emergency
- Challenges to the Security Program from Outside and Inside Sources

Countermeasure goals and functions are presented in Figure 15.4.
### Countermeasure Goals and Functions (Examples)

<table>
<thead>
<tr>
<th>Countermeasure Goals</th>
<th>Countermeasure Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identify and Deny</strong></td>
<td><strong>Access Control</strong></td>
</tr>
<tr>
<td><strong>Access to Potential</strong></td>
<td><strong>Deterrence</strong></td>
</tr>
<tr>
<td><strong>Threat Actors</strong></td>
<td><strong>Detection</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Assessment</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Delay</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Response</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Evidence</strong></td>
</tr>
<tr>
<td>Access Control,</td>
<td>Visible Devices,</td>
</tr>
<tr>
<td>Screening Posts,</td>
<td>Guards, Dogs, and</td>
</tr>
<tr>
<td>and Employee</td>
<td>Alarm Devices Including</td>
</tr>
<tr>
<td>Screening</td>
<td>Security Awareness</td>
</tr>
<tr>
<td></td>
<td>Motion</td>
</tr>
<tr>
<td></td>
<td>Console, Guards,</td>
</tr>
<tr>
<td></td>
<td>and Security Awareness</td>
</tr>
<tr>
<td></td>
<td>Policy</td>
</tr>
<tr>
<td></td>
<td>Operable Barriers</td>
</tr>
<tr>
<td></td>
<td>and Guard Posts</td>
</tr>
<tr>
<td></td>
<td>Console, Guards,</td>
</tr>
<tr>
<td></td>
<td>Operable Barriers and</td>
</tr>
<tr>
<td></td>
<td>Intercoms</td>
</tr>
<tr>
<td></td>
<td>CCTV, Intercoms,</td>
</tr>
<tr>
<td></td>
<td>and Witness Reports</td>
</tr>
<tr>
<td><strong>Deny Access to</strong></td>
<td>Screening, Guard</td>
</tr>
<tr>
<td><strong>Weapons, Explosives,</strong></td>
<td><strong>Posts, and</strong></td>
</tr>
<tr>
<td><strong>and Dangerous</strong></td>
<td><strong>Procedures</strong></td>
</tr>
<tr>
<td><strong>Chemicals to the</strong></td>
<td><strong>Procedures</strong></td>
</tr>
<tr>
<td><strong>Facility</strong></td>
<td><strong>Detectors, Dogs,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Guards, and</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Procedures</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Screening Posts, Dogs,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>and Patrols</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Operable Barriers and</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Guard Posts</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Console, Guards,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Operable Barriers and</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Intercoms</strong></td>
</tr>
<tr>
<td></td>
<td><strong>CCTV, Intercoms,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>and Witness Reports</strong></td>
</tr>
<tr>
<td><strong>Make the Environment</strong></td>
<td>CPTED Design, <strong>Policies</strong></td>
</tr>
<tr>
<td><strong>Suitable for</strong></td>
<td><strong>and Procedures,</strong></td>
</tr>
<tr>
<td><strong>Appropriate Behavior</strong></td>
<td><strong>Training Programs, and</strong></td>
</tr>
<tr>
<td><strong>and Unsuitable for</strong></td>
<td><strong>Security Awareness</strong></td>
</tr>
<tr>
<td><strong>Inappropriate for</strong></td>
<td><strong>Programs</strong></td>
</tr>
<tr>
<td><strong>Criminal or</strong></td>
<td><strong>Policies and</strong></td>
</tr>
<tr>
<td><strong>Terroristic Behavior,</strong></td>
<td>**Procedures, **</td>
</tr>
<tr>
<td><strong>and to Mitigate the</strong></td>
<td><strong>Training</strong></td>
</tr>
<tr>
<td><strong>Actions of Both</strong></td>
<td><strong>Programs</strong></td>
</tr>
<tr>
<td><strong>Hazards and Threats</strong></td>
<td><strong>Security</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Awareness Programs</strong></td>
</tr>
<tr>
<td>Patrols and Reports</td>
<td>PatROLS and Reports by</td>
</tr>
<tr>
<td>by Organization</td>
<td>Organization Members</td>
</tr>
<tr>
<td>Members</td>
<td></td>
</tr>
<tr>
<td>See Above</td>
<td></td>
</tr>
<tr>
<td>CCTV, Intercoms,</td>
<td></td>
</tr>
<tr>
<td>and Witness Reports</td>
<td></td>
</tr>
</tbody>
</table>

**FIGURE 15.4 Countermeasure Goals and Functions**
SUMMARY

Security countermeasures are measures that are taken to counter a threat action. Ideally, security countermeasures would be so effective as to completely eliminate the will of potential threat actors to take action. Countermeasures should be focused on both security measures but also on being balanced with the needs of the organization’s daily business needs. Compromises are always necessary.

All security countermeasures have the broad goal of adjusting the behavior of potential threat actors so that they do not pose a threat to the organization. This is done in three ways:

1. Design an environment that encourages appropriate behavior and discourages inappropriate, criminal, or terrorist behavior.
2. Detect, assess, and respond to exceptions.
3. Design the program to mitigate any potential harm from hazards and threats.

Implementation strategies include:

- Control access to the target, denying access to possible threat actors.
- Deter any threat action from occurring.
- Detect any threat action.
- Assess what has been detected.
- Respond to any active threat action.
- Gather evidence for prosecution, investigation, and training.
- Comply with the business culture of the organization.
- Minimize any impediment to normal business operations.
- Help to create an environment where people feel safe and secure and can focus on the purpose of the organization.
- Design programs to mitigate possible harm from hazards and threat actors.