The Hanover Insurance Group®

Hanover Risk Solutions

Security for Computer Facilities

Computer security can be defined as the protection of all computer assets, including the facility, equipment (hardware), programs (software), and information (data), from theft, alteration, or destruction due to manmade and natural hazards. This report discusses the elements of a basic security program for a computer facility.

Computer systems are susceptible to damage or destruction from many sources. Damage can result from a malicious act or natural disaster, or may be due simply to carelessness on the part of an operator. The system can be impaired by fire, flood, wind, or earthquake, or destroyed by the collapse of the building in which it is located. Data can be erased by a failure to follow established procedures or by the introduction of viruses. Vital information can be stolen by industrial espionage. Systems are at risk from disgruntled employees who, for revenge, may sabotage tapes or hardware; from hackers who trespass into systems for "fun" and "crackers" (criminal hackers) who do it for financial gain; and from militant groups or terrorists who may view a facility as a desirable symbolic target.

Computer security can be defined as the protection of all computer assets, including the facility, equipment (hardware), programs (software), and information (data), from theft, alteration, or destruction due to manmade and natural hazards. The level of security needed for a particular computer system depends on a number of factors: the environment and facility in which the system operates (e.g., whether it is a Defense Department contractor or a university research laboratory); the type of equipment and its telecommunications links; the computer programs used; the type of information stored or processed, and its sensitivity; and the people involved.

This report discusses the elements of a basic security program for a computer facility. These elements are protection from nature, physical security, disaster planning, employee selection, and security auditing.

Site Selection and Protection

The location of the computer facility should be carefully analyzed to minimize potential damage from hazards, such as fire, windstorm, flooding, explosion, and earthquake. Proper site selection will help to limit the likelihood of serious loss from these hazards.

Fire

Fire is one of the most serious threats to a computer system. Not only is fire a direct cause of loss, but it can occur as a consequence of other disasters, such as earthquakes, floods, or explosions. An evaluation should be made of the fire safety

continued ▸

of the facility with regard to its location, construction, occupancy, and housekeeping so that the proper fire detection and extinguishing systems can be provided. Requirements for the protection of electronic computer equipment, components, and associated records from fire are provided in NFPA 75, *Standard for the Protection of Information Technology Equipment*, published by the National Fire Protection Association (NFPA). See also, Fire Protection Report FP-23-03, *An Overview of Extinguishing Systems for Computer Equipment*.

Windstorm

The building in which the computer system is housed should be designed to resist maximum anticipated wind forces. Hurricanes, tornadoes, and cyclones all represent potential threats to a computer facility. Historical weather data for an area is available, such as from the National Oceanic and Atmospheric Administration and the local office of the National Weather Service.

The building should not be located where it would be subject to damage from collapsing trees, masts, towers, or metal stacks. Windows on exterior walls should be eliminated, when feasible, since they can be broken by windblown debris, resulting in the exposure of equipment to wind-driven rain. Alternatively, the windows can be retrofitted with plastic laminates that have been tested and listed by Underwriters Laboratories Inc. (UL). These plastic laminates are designed to maintain the integrity of the window in the event the glazing is broken, thus reducing damage from wind-driven rain. A number of building codes have provisions for protecting buildings from damage due to windstorms.

Flood Damage

Areas where rivers and waterways are known to overflow are undesirable locations for computer facilities because of the potential for flood damage. Floods are more likely to occur in river and flood plains where they can be caused by heavy rainfall, snow-melt runoff, or obstruction of a narrow channel; in coastal flood plains where they can result from high tides, wind-driven waves, tsunamis (large waves caused by undersea earthquakes or volcanic eruptions), or a combination of these effects; and at the base of a mountain where debris cones deposited by mountain streams can suddenly give way, resulting in flash floods. Flood hazard information is primarily available from the Army Corps of Engineers.

Water damage can also occur from other sources, such as burst water pipes and clogged drains on roofs. For this reason, the location of the computer facility within the building must also be evaluated. A basement is the least desirable location for a computer operation because of its potential to collect water. Basement drains can be provided with check valves to prevent backup, and sump pumps can be utilized to augment natural drainage; however, in an emergency, all these measures may prove ineffective. Roofs should be properly maintained and drains and down spouts cleaned on a regular basis to prevent clogs.

The ceiling and floor above the computer facility should be inspected for plumbing lines and holes. Ideally, no plumbing lines should be routed through the facility, except for fire protection purposes, and all holes in the floor slab should be sealed. It is highly recommended that all computer facilities be

stockpiled with plastic sheets that can be used to protect equipment in an emergency.

Almost all computer facilities are designed with a raised floor to provide a protected space for inter-cabinet and power cables and as a supply air plenum for the air-conditioning system. If water collects in this space, there is a risk of electrical short-circuiting and corrosion to equipment. This space should be provided with positive water drainage.

Explosion

Exposure to potential sources of an explosion can be limited by avoiding locating the computer facility directly above or adjacent to boiler rooms, compressor rooms, hot water tanks, and laboratories or process areas that handle flammable or combustible liquids or gases. Piping for combustible liquids and gases and high pressure gas mains should not be routed through, or located over, under or adjacent to, the computer facility. Where an explosion hazard exists from other properties or tenants, the computer facility should be located as far away as practicable from the exposure.

Earthquakes

Earthquakes represent a threat to computer operations because of the potential for structural damage or collapse of the building, interruption of electrical or communications circuits, and loss of utilities. Assessing the probability of an earthquake occurring in an area is difficult because of the relatively short recorded history of seismic events in the United States. However, information on the long-term hazard, as well as the probable severity of earthquakes in a particular area, is available from the National Earthquake Information Center.

Potential damage from earthquakes can be limited by building design and proper site selection. In susceptible areas, the building should be designed to be earthquake-resistant. Locations that should be avoided include fault lines, hillsides, landfill areas, waterfront areas, fuel storage areas, and in the vicinity of tall structures that could potentially collapse on the facility.

In general, the means for limiting potential damage to a computer facility due to the occurrence of a fire, hurricane, or earthquake, among other considerations, are provided in model building and fire prevention codes and standards. The latest editions of these codes and standards provide information necessary for the proper design and construction of a building to resist these hazards.

Building Security

Physical security involves the protection of the computer facility and hardware from damage or destruction due to manmade hazards. Manmade hazards include industrial espionage, sabotage, riots or civil unrest, vandalism, and theft.

In response to the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995, the federal government developed a set of security standards for federal buildings. The standards cover perimeter security, entry security, interior security, and security planning and may be applicable to computer facilities. The standards are provided in the report, *Vulnerability Assessment of Federal Facilities*, which is available from the U.S. Government Printing Office, Superintendent of Documents, Mail Stop: SSOP, Washington, D.C. 20403-9328; Stock Number 027-000-01362-7.

Fencing

For high-security facilities, the perimeter of the property should be protected by a fence or other physical barrier to deter intruders. A chain-link fence should be of at least 9-gage wire and a minimum of 8 ft. (2.4 m) in height. It should be provided with a top guard consisting of three strands of barbed wire mounted on metal supporting arms that extend upward and outward, depending on local laws, at an angle of 45°. The bottom of the fence should be provided with a bottom rail or 7-gage tension wire to prevent "rolling up" the bottom of the fence. Gates should be securely mounted and provided with a top guard.

During non-business hours (if the entrance is not manned by security personnel), gates should be adequately secured. A gate should be locked with a true hardened chain and heavy-duty padlock that is installed in such a manner as to limit the potential for attack from outside the property.

Crime Prevention Report CP-31-10, *Chain-Link Fencing*, provides information on the design and construction of chain-link fencing. The nationally recognized standard for chain-link fencing is ASTM F567-91, *Practice for the Installation of Chain-Link Fence*, which is published by the ASTM International, Inc. (ASTM). The standard provides requirements for the manufacture, design, and installation of chain-link fencing.

Depending on the level of security desired, a fence can be provided with an alarm system. The alarm system can be designed and installed to detect attempts to climb over, cut through, or tunnel under the fence.

Lighting

To discourage intruders, the property should be well lighted at night. Fixtures should be installed high, out of reach of intruders, and should be of the vandal-resistant type. A maintenance program should be instituted to ensure that burned-out lamps are replaced on a timely basis.

Crime Prevention Report CP-32-10, *Protective Lighting Systems*, discusses the principles of protective lighting systems and considerations in the use and operation of different types of lighting fixtures. Information on recommended lighting levels for specific areas or locations is provided in the *Guideline for Security Lighting for People, Property, and Public Spaces*, IESNA G-1-03, published by the Illuminating Engineering Society of North America.

Security Guards

Depending on the level of threat to the facility, guards should be stationed at the main building entrance(s) and/or gate(s) during business hours to control the access of people and/or vehicles. During non-business hours, guards should patrol the facility.

Background checks should be performed on all guards (private security officers). Guards should be properly trained in the legal and practical applications of their jobs. Guard patrols should be supervised to assure that patrols are being performed as required. Local and/or State laws may have specific requirements for the selection and training of security guards. Information on the selection, training, and licensing of guards is provided in Crime Prevention Report CP-71-10, *Guidelines for the Selection, Training and Licensing of Private Security Officers*.

Perimeter Protection

Good perimeter protection is most easily accomplished in buildings with the following construction features: walls, floor, and roof of reinforced concrete; no exterior windows; the number of exits limited to only those necessitated by life safety and building code requirements; and solid exterior doors that will resist physical attack. This type of construction alleviates many of the problems associated with unauthorized access, including exterior bombing attacks and forced entry attempts. For a more complete discussion of building protection, see Crime Prevention Report CP-30-10, *Physical Protection Afforded by Buildings*.

Besides doors and windows, the perimeter of the building should be checked for other openings, such as air conditioning louvers, vents, transformer vaults, roof hatches, and the like. These all represent potential points of illegal entry and should be provided with protection. Windows can be bricked up with glass blocks or the glass replaced with burglary-resisting or attack-resistant glazing materials (see Crime Prevention Report CP-38-20, *Burglary- and Forced-Entry-Resisting Glazing Materials*). Louvers and vents can be protected with heavy-gage screens. Roof hatches can be secured on the inside with a padlock and hasp. Transformer vaults can be completely enclosed with chain-link fencing. In those cases where physical protection of the opening is impractical, the opening can be provided with burglar alarm system protection.

Access Control

The key to protecting a computer facility from manmade hazards is access control—that is, permitting access to the facility by authorized persons while denying access to others. Depending on the layout of the facility, access control should be provided in the following areas: the perimeter of the property; public entrances and loading docks; the data processing areas; the computer room; and the communication, air conditioning, and electrical equipment areas.

From the standpoint of security, the best location for a computer operation is in a separate building used only for that purpose. In a single-purpose building, it is easier to set up and maintain physical access controls and intruders become more conspicuous. However, it can be argued that a separate building makes the computer facility more vulnerable to terrorist attack. Alternatively, the facility could be located on a separate floor in a building or in a physically-separated area of the floor that allows for access to be controlled.

Access into the facility should be controlled by a card access control system that requires the use of a card and Personal Identification Numbers (PINs) or biometric information for entry. All employees should be provided with photo-identification badges that are required to be worn at all times. Visitors should be logged in and escorted to the person they are visiting. Similar procedures should also be followed at loading docks. Information on access control, in general, is provided in Crime Prevention Report CP-93-10, *Security for Office Buildings*, and, specifically, for card access control systems in CP-33-10, *Card Access Control Systems*.

Computer systems rely heavily on controlled temperature and humidity, as well as a continual supply of electric power, for proper operation. Sabotage or vandalism to these utilities can cause an operational shutdown of the system and the resultant business

interruption. Access into these areas must be restricted to only maintenance personnel and other authorized persons, to limit the potential for sabotage or vandalism. Intrusion detection systems and closed circuit television will provide additional levels of protection.

Alarm Systems

Even if the computer facility operates 24 hours a day, seven days a week, there may be times when sensitive or critical areas of the facility will be vacant and unsupervised. Besides the usual physical security measures, such as strong doors and good locks, these areas should be provided with an alarm system and/or closed circuit television system to detect the presence of intruders and limit the opportunity for fraud or sabotage by unauthorized personnel. The alarm system should consist of contacts on all doors, especially emergency exits, to monitor their opening, and motion detectors installed throughout the area to detect movement. The alarm system can be tied into a closed circuit television system so that, on activation of the alarm system, guards can view the area from a remote monitoring location. The alarm system should be continuously monitored at a central station or proprietary station.

Closed Circuit Television

Closed circuit television (CCTV) can be used in a computer facility for security surveillance, access control, and alarm monitoring and detection. As a surveillance device, CCTV can be used to monitor hallways, parking lots, and other areas. In access control, it can be used as an aid in identifying visitors requesting entry. And in alarm monitoring and detection, a video motion detector can be used to detect unauthorized intruders. For a discussion of the application of CCTV, see Crime Prevention Report CP-52-20, CCTV – *Application and Use*.

Sabotage

As the use of computers in the business world has increased, there has arisen such a demand for experienced computer personnel that many companies, in hiring these workers, often forego the background checks and hiring procedures that are standard practice in the company. However, these workers also have the best opportunity to sabotage, or otherwise damage, the computer system. The best facility security program is of little value if the perpetrator (criminal) can gain entry in the guise of an employee. The screening process is a basic component of any computer security program and, as such, should not be sidestepped in the search for qualified people.

Liability Report LB-70-50, *Interviews and Background Checks*, provides information on the options that are available to employers in screening job applicants and the limitations, imposed by federal and state privacy laws, on the ways in which employers can use this information.

Disaster Planning

Despite the precautions taken to limit losses from natural and manmade hazards, the possibility still exists for events to take place that may interfere with the normal operation of the computer facility. For this reason, contingency plans must be established for those instances when protective systems fail or are overcome by nature or other events. The contingency plan should include the following:

- Emergency response procedures in the event of a fire, flood, civil disorder, or bomb threat in order to protect lives, limit the damage to property and minimize the impact on computer operations.

- Back-up operation plans to assure that essential tasks can be completed and operations continued, either on-site (if there is only a partial loss of capability) or off-site (if there has been major damage or destruction).
- Recovery plans to permit rapid restoration of the computer facility following major damage.

For a complete discussion of disaster planning, see the following Natural Hazard Reports:

NH-30-10, *Emergency Preparedness—An Overview*

NH-30-11, *Emergency Preparedness—Developing the Plan*

NH-30-12, *Emergency Preparedness—An Example Plan*

NH-30-13, *Emergency Preparedness—Recovery Operations*

NH-30-14, *Emergency Preparedness—Protecting Vital Records*

Auditing

Once a system of security controls and procedures have been implemented, it becomes necessary to perform regular audits to assure that controls are functioning as intended and to discover violations of the controls. The audit should accomplish the following objectives:

- Evaluate the security controls for the facility.
- Provide management with the opportunity to improve and update its security program.
- Provide the impetus to keep employees and management from becoming complacent.
- Uncover areas of vulnerability.

An important consideration in establishing an audit program is the makeup of the audit team. The team should be composed of personnel who do not have responsibility for computer operations and are outside the span of control of the security department or manager; otherwise, the computer or security staff would be performing an audit of its own functions. Members of the audit team should have some training in computer systems—a programming or operations background is desirable—and knowledge of basic auditing principles. Expertise in either area is not essential, since the objective of the team is to evaluate the adequacy of established controls and procedures, not to develop them.

References

1. Federal Emergency Management Association. Emergency Management Guide for Business & Industry. Washington, DC: Department of Homeland Security, 2004. http://www.fema.gov/media-library/assets/documents/3412
2. Federal Emergency Management Association. Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings. Washington, DC: Department of Homeland Security, 2005. http://www.fema.gov/media-library/assets/documents/4608
3. National Institute of Standards and Technology (NIST). An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12. Washington, DC: U.S. Department of Commerce, 2002.
4. U.S. Department of Justice. Vulnerability Assessment of Federal Facilities. Stock number 027-000-01362-7. Washington, DC: Government Printing Office, 1995.

The Hanover Insurance Group®

The Hanover Insurance Company
440 Lincoln Street, Worcester, MA 01653

hanover.com

171-0921 (9/16) LC 11-126 May 2011