Basic Security Planning in the Office Environment

A Checklist for Assessing Physical Security Needs

By
Randy Gonzalez

www.drgonzo.org

Introduction

An accurate measure of the dollar losses experienced each year by American businesses is very difficult to establish. The amount, however, represents a significant figure, which has been estimated in excess of $100 billion on an annual basis. This figure has been suggested by researchers in field to be on the conservative side. The actual amount of yearly losses may in fact be much greater. Losses attributed to theft, inventory shrinkage, employee pilferage, computer related crimes, fraud and embezzlement continue to increase each year, and seriously impact our nation's businesses with alarming frequency.

Unfortunately, many business executives refuse to consider that they may have a security problem, which will eventually lead to dollar losses, or perhaps injury to personnel. Some business managers do not want to believe that their employees would steal, or that an analysis of their business operations may reveal security weaknesses. While it is probably impossible to safeguard all corporate assets 100% of the time, there are basic steps that can be taken to reduce the opportunity for a crime to occur.

The following checklist is designed to provide basic information to assist in the development of a business loss prevention program. This information focuses on the office setting, following accepted crime prevention principles. It should be kept in mind that no two business operations are exactly the same, and the checklist should be considered as a flexible tool that should be modified when necessary to fit the needs of the specific business facility. These guidelines are offered to assist the business excutive in reviewing present operations and procedures, to identify potential weaknesses. Every business executive should begin now to analyize and assess his or her business security environment, and inventory potential vulnerabilities.

Protecting the Office Area

This purpose of this part of the overall checklist, which includes the topic areas that follow, is to alert the business person as to possible security problems within the office or work environment. A "yes" response to a question indicates that further analysis and attention will be required to fully address an existing physical security problem.

1. Is it possible for an unauthorized person to enter and leave the office or work area without contact with office personnel, receptionist, etc.?
2. Is it possible for an unauthorized person to gain access to equipment storage rooms without being detected by office personnel?
3. Are access points, such as windows, doors, etc., routinely and properly secured?
4. Is at least one member of the office work group assigned responsibilities for securing all doors, windows, etc., after normal business hours?
5. Does someone have the responsibility to inventory all office equipment at least once a year?
6. Is a duplicate inventory list filed at another location in a secure place, in the event the original list is lost, stolen, or forged?
7. Are appropriate records kept when property is sent out for repair?
8. Are photographs kept on file for identification purposes of high value office equipment?
9. Are there written company policies with regard to office equipment that is loaned or otherwise used outside the office?
10. Are procedures and polices regarding the use of office equipment routinely enforced and followed by all personnel?

11. Is office equipment engraved or otherwise marked in at least two places with some form of identification number?
12. Is it possible to remove any office equipment during normal business hours without being observed by office personnel?
13. Is high risk office equipment stored in a locked file cabinet or storage area after normal business hours?
14. Is office equipment, such as typewriters, secured to a fixed object, or anchored to a desk, etc., to prevent unauthorized removal?
15. Is the copy-machine well supervised to prevent unauthorized use?
16. Is a list kept on file of all personnel who have keys to equipment storage areas, supply rooms, etc.?
17. Are keys to the building and internal building areas strictly controlled and accounted for on a regular basis, such as once a year?
18. Is an inventory or log maintained on all personnel who are issued keys?
19. Does the key inventory or log specify the number and type of locations each key will allow access?
20. Has a personal safety program been developed for all office personnel, especially those who work late at night?

Protecting the Computer Room

As more and more businesses replace their manual records and reports with data processing systems, the protection of business information, including confidential business aspects, becomes even more critical. Management control of internal operations becomes more difficult, with the possibility of surreptitious entry into an information system. No single set of guidelines will provide all the information necessary to give the business executive 100% foolproof protection for his or her computer facility. Volumes of information

have been written in recent years covering the many complex issues related to information security, as well as physical security, for a computer operation. The following list presents some of the basic safeguards that should be considered, in order to reduce the opportunity for a breach of security with regard to the computer facility. The major emphasis expressed in this listing pertains primarily to physical security.

1. Have company policies and procedures regarding security of the computer facility been established in writing, and are all personnel aware of the policies and consequences following a breach of security?
2. Has a security policy regarding passwords and confidential information been developed?
3. Are personnel within the computer facility periodically tested as to their knowledge of security policies and procedures?
4. Is access to physical assets and data effectively restricted to authorized personnel by electronic and physical controls?
5. Is a regular inventory conducted of data communications equipment, including terminals, modems, etc.? All facility equipment?
6. Has the company established a well defined personnel screening program in order to conduct background checks on potential employees for the computer facility?
7. Is there a disaster recovery plan and a back facility available in the event of an emergency?
8. Are all breaches of security, whether actual or suspected, immediately brought to the attention of the security department and/or management?
9. Are current operations, procedures, etc., consistent with company policy?

10. Is a key control inventory maintained for all personnel who have keys to any part of the computer facility?
11. Is an alarm system in use for the computer facility to control access, as well as protect the facility?
12. Is there an established procedure for authorization in the use of the computer facility after normal business hours?
13. Is there a dialogue between user and the computer system for the purpose of identification and authorization at all times?
14. Are users assigned unique user identification codes?
15. Are passwords assigned to verify users?
16. Are passwords and identification codes changed periodically, with regard to sensitivity of application?
17. Are secondary identifiers, such as cardkeys, used to identify and authenticate terminal users in addition to, or instead of, passwords?
18. If a user develops his or her own password, is there a program or other means to review each password to ensure that it is not a copy of the user's name, birth date, etc.?
19. Is the computer file librarian provied with a list of which personnel are permitted to withdraw what files?
20. Are authorized personnel limited to designated files and restricted to the program operations they may perform?
21. Are software security programs used to restrict authorized users to certain files, sections of files, etc.?
22. Do remote terminals contain lockable keyboards, locks on terminal on/off switch, etc.?
23. Has every effort been made to physically secure the computer room or facility?

24. Are procedures used to ensure that terminal users log-off before leaving a terminal, and that they remove all paper, including carbons, or ribbons, which should not be seen by other users?
25. Is it possible for a terminal user to work in privacy to prevent other unauthorized persons from observing passwords, identification codes, etc.?
26. Have phone lines been protected to screen unauthorized dial-up to the computer facility? Phone number changed periodically?
27. Is the computer library well protected against unauthorized entry, and is a log kept requiring an authorized signature for any materials that are checked out?
28. Is the computer library maintained in a secure area separate from the computer room?
29. Are data files protected under the supervision of security personnel or management, rather than user areas?
30. Is the computer facility security plan periodically reviewed and updated?

These several aspects of protecting the computer operations cover only the basics of planning security for data processing operations. Every effort should be made to fully examine present facilities and operations in detail. A comprehensive analysis, along with a well designed security program, should be developed as soon as possible. It is recommended that the business executive investigate the current research and literature available in the field of computer security.

Protecting the Business Office Location

Building security is important to any business operation. The crime prevention principles of access control, locks and hardware devices, con-

struction, and other aspects of security planning should be thoroughly analyzed with regard to overall building security. Depending on the design, location, size and use of the building facility, the security plan will vary, along with the security needs of the business operation. No two building sites, with regard to security situations, will be identical. The safety and security requirements of personnel and property will depend also on the extent to which a particular business controls a particular building. A business, for example, may occupy an entire building facility. In this case, physical security planning for the entire structure may be easier to accomplish. However, many businesses may share one building facility, with vertical occupancy of the structure composed of many tenants performing unrelated business activities. In this situation, security planning may be more difficult without cooperation and assistance from all tenants.

The following information pertains mainly to multi-level buildings. For the purposes of discussion, it is assumed that some collective control over security planning is possible, regardless of the number of business tenants in the high-rise building facility. This information covers the basic aspect of high-rise building security planning.

1. With regard to the high-rise building's exterior, do surrounding buildings or the neighborhood present observable security hazards?
2. Has an examination been conducted of the perimeter barriers in order to control unauthorized access (e.g. doors, windows, fire escapes, basements roof hatches, and other access routes)?
3. Is it possible to gain access by compromising such things as doors, door hinges and pins, locks, stairwells, elevators, etc.?

4. Are side, rear, alley way entrances, (those removed from public view) protected to prevent unauthorized access?
5. For building access points or openings which require a locking device, have these been routinely examined to ensure proper operation?
6. Is proper security hardware, such as deadlocking devices, used on all such openings (when permitted by local fire code)?
7. Do doors fit properly within the frame, and do door locks bolt snuggly into the jamb? Would prying be easy to accomplish?
8. Has the exterior lighting of the building been recently examined to ensure a proper level of nighttime lighting?
9. Has lighting been examined for such areas as alleys, fire escapes, service areas, etc.?
10. Does exterior and interior lighting enable police, security personnel and the public to detect a possible instruder?
11. Is exterior lighting controlled by an automatic system, or is someone required to mannually operate the lighting after business hours?
12. Is exterior lighting consistent with recommended standards for safety and security? Such as the following examples: (minimum)

Situation:	Suggested Lighting Levels (Footcandles):
Pedestrian Walkways	5 fc.
Pedestrian Entry & Access Points	5 fc.
Pedestrian Street Crossings	8-10 fc.
Surface Parking	5 fc.
Garage Stairwells & Elevator Lobbies	15 fc.

13. Is the exterior building perimeter protected by an intrustion detection system? If so, is the system routinely inspected and maintained?
14. Do employees, elevator operators, maintenance personnel assist in maintaining vigilance of the premises for unauthorized persons, etc.?
15. Is there a training program for employees, service personnel, etc. to assist in the security program?

16. For sensitive areas within the building (computer rooms, confidential file storage, etc.), is there an employee identification system, such as company issued cards or badges?
17. Is employee parking provided? If so, is there a security program for personal safety?
18. Is parking provided for company vehicles? If so, is there a security program for safeguarding the vehicles (i.e. theft of parts, vehicles, etc.)?
19. Is there a program that controls access to the building, particularly sensitive areas, by contractors, vendors, repairmen, janitors, etc.?
20. Does the building have a security patrol? If so, what is their level training, policies, procedures for dealing with security problems, etc.?
21. Are security patrol routes varied with regard to times and coverage of sensitive areas? Could a potential intruder determine their routine?
22. Are corporate mail rooms adequately protected?
23. Are corporate record keeping facilities adequately protected?
24. Are safes and vault rooms protected? Are combinations regularly changed, especially when an employee transfers or resigns? Is a log maintained of all persons who have combinations and access to safes or vault rooms?
25. Who has primary responsibility for the physical security of the building? Is there liaison with local law enforcement?
26. Is the loading dock well lighted and controlled as a possible access point to unauthorized persons?
27. Is the loading dock a trash collection point for building paper wastes? If so, has paper been shredded with regard to sensitive corporate information? Are trash collection areas inspected to ensure property or company records, etc. are not concealed for later removal?

28. Is the power system, mechanical rooms, and auxiliary power equipment well protected to prevent tampering or sabotage?

29. Are elevators protected to prevent access to the elevator shafts, or elevator equipment? Are elevators restricted from certain floors containing sensitive operations after normal business hours?

30. Are executive suite levels adequately protected, such as an arrangement with a lobby and receptionist so that stairwells and elevators can be observed? Can the receptionist summon security personnel or the police in the event of an emergency situation?

31. Does the building design and layout, including surrounding exterior areas adjacent to the building's premises, foster a feeling of safety on the part of customers and personnel? Does it promote security surveillance?

32. Does the facility create physical and psychological barriers which serve to warn a potential intruder, thereby creating the perception of increased risk of detection?

33. Do long hallways, hidden stairwells, and long elevator systems create conditions for criminal activity?

34. Does landscaping create a positive environment that suggests a crime-free attitude on the part of the tenants? Are shrubs and lawns well trimmed to reduce places of concealment, and promote safety and security? Does landscaping promote a sense of territoriality on the part of the tenants?

35. Is there good communication among the building's tenants, and do all the businesses take part in the security planning program?

Summary

Proper business security planning in the office environment is an essential part of good business practices. The checklist presented covered three primary areas of business concern for physical security planning: the individual office area; the computer operations; and the overall business building or high-rise facility. The items presented only addressed the basic areas of a business security program within a non-retailing or non-industrial environment. A comprehensive security plan should begin with the items presented in the previous pages. However, it should be kept in mind that this is not an exhaustive list of the many physical security aspects that would be the final product of an extensive physical security program. In order for the business executive to establish a good physical security program, he or she must first accept the fact that no matter how effective he or she manages, there is always the potential for criminal activity. Anticipating that a crime will occur at some point in the future, is a basic element of crime prevention planning. Recognition of potential security problems, through the use of the checklist presented, serves as the next basic step in reducing potential risks to the business. An appraisal of current operations and conducting an inventory of vulnerabilities, assist in making decisions with regard to safeguarding property and personnel. Finally, initiating positive action to remedy existing security problems serves to reduce the opportunity for a crime to occur.