Homeland Security

Tools for Small Business

ACKNOWLEDGMENTS

The Risk Management Small Business Development Center wishes to express its special appreciation to the U.S. Small Business Administration for sponsoring this publication. This project allowed us to provide critical information to the small business owners of the United States of America about their role in providing Homeland Security throughout our nation.

Others who provided invaluable assistance as they always have in the past are:

SBA, Office of Small Business Development Centers

Liz Klimback, Regional State Director, North Texas Small Business Development Center Regional Headquarters, Dallas, Texas

Don Wilson, President, Association of Small Business Development Centers

Donna Ettenson, Vice President Operations, Association of Small Business Development Centers

Cheri Hebison, EOSH Coordinator, Risk Management Small Business Development Center

Saira Roberts, Administrative Assistant, Risk Management Small Business Development Center

Mireya Martinez, Administrative Assistant, Center for Government Contracting

Katrina Wade-Miller, MIS Director, North Texas Small Business Development Center

Yvonne Robertson, North Texas Small Business Development Center Regional Headquarters

This book and the associated SBDC counselor training program can be downloaded at:
www.ntsbdc.org or at www.asbdc-us.org

Cover photograph provided by NASA without copyright under the name City Lights. See web-sites http://photojournal.jpl.nasa.gov/catalog/PIA02991 or http://visibleearth.nasa.gov/cgi-bin/viewrecord?5826

Photograph on Chapter number pages is provided by William L. Weddle Jr. (Copyright 2004)

Risk Management Small Business Development Center, *Publisher*

William L. Weddle, Jr., Director, Risk Management Small Business Development Center, *Managing Editor / Author (214) 860-5821 or wlw9515@dcccd.edu*

Cheri V. Hebison, Risk Management Small Business Development Center, *Contributing Writer / Editor*

Saira Roberts, Risk Management Small Business Development Center, *Contributing Writer / Editor*

The information in ***Homeland Security: Tools for Small Business*** was compiled as of September 2004 and is therefore subject to change without notice as new technology and information becomes available. While every reasonable effort has been made to ensure that the information contained herein is accurate as of publication date, none of the Risk Management Small Business Development Center (RM SBDC), North Texas Small Business Development Center (NT SBDC), the Small Business Administration (SBA), nor any of their employees, agents, clients, members and distributors shall be liable for any damages arising from the use of or reliance on the information contained in this book or from information that may not be included in this book.

The listing of organizations, products, corporations and/or services in this publication is provided for the convenience of users of this book and does not constitute an overt or implied endorsement by the Risk Management Small Business Development Center, the North Texas Small Business Development Center, the Small Business Administration, it employees, sponsors, partners, distributors or members and should not be construed as such.

The Risk Management Small Business Development Center is solely responsible for all information contained in this book.

The views and policy interpretations expressed in this work by the authors are their own and do not necessarily represent those of any of its subsidiaries, business units or affiliates.

CONTENTS

Chapter 2

- Areas of Concern - Inner Layers (Facility)
  - Unauthorized Entry
  - Theft
    Substance Abuse
    Trade Secrets
    Intellectual Property
  - Disgruntled Employee
    Contractor Actions
    Workplace Violence
  - Material Contamination
    Equipment Damage
    Production Stoppage
    Sabotage
    Terrorist Acts

- Intrusion Prevention
  - Offices and People Flow Arranged for Visibility
  - Visitors by Appointment with Sign-in and Escort
  - Locks on all Gates and Doors
    - With Serial Numbers Removed
  - Access Control System with Audit Trail
    - Photo ID with Mandatory Check-in
    - Electronic Keypad of Card Swipe
    - Biometric ID
  - Video Surveillance
  - Vehicle Entry Permission System
    - Cars, Trucks, Rail or Boat
  - Receiving and Inspection Process
    - Located near Entrance
    - Separate Ventilation/Area can be Isolated
    - Easily and Thoroughly Cleanable
    - Mail/Parcels
    - Raw Materials
    - Equipment and Supplies
    - Product Sample

- Limiting Damage - Potential Targets

  (Plant and Equipment)
  - Well Designed Barriers Against Vehicles
  - Blast Resistant Buildings or Structures
  - Design Layout to Limit Accessibility

  (Chemicals and Chemical Storage Containers)
  - Valves and Pumps Inside Buildings or Fences
  - Excess Flow Check Valves
  - Overfill Protection
  - Fail-Safe Design
  - Breakaway Couplings
  - Adequate Containment Systems
  - Double-Walled Tanks
  - Chemical Monitors
  - Compressed and Liquefied Gases

  (Communications and Computers)
    - Provide Security in Layers
    - Access Control
    - Physical Breaking and Entry
    - Hacking (Internal and External)
    - Firewall and Continuously Updated Security Software
    - Intrusion Detection (Physical and Digital)
    - Password Control
    - Back-up Power Systems
    - Alternate Systems for Confidential Information
    - Off-Site Back-up and Disaster Recovery Equipment
    - Emergency Radios and Cell Phones

  (Personnel - Full-Time, Part-Time, Temporary and Contractors)
  - Use Aggressive Background Checks
    - 80% of Network Security Breaches from Inside
    - 18% of Applicants Lie About Criminal Records
    - 29% Lie About Education History
    - 25% Misrepresent Employment History
    - 23% Have Used Other Names in the Past
  - Drug Screening
    - 74% Of Drug Users Are Employed PT Or FT
  - Pre or Post Hire Physicals
  - Zero Tolerance Termination for False Information

Chapter 3

- **Procedures and Policies**
  - Posted Security Plan
  - Incident Reporting System
    - Investigation
    - Trends
    - Corrective Actions
  - EPA Risk Management Plan
    - Section 112(r) Clean Air Act
- OSHA General Duty Clause
  - Labor Relations
  - Workplace Violence
  - Substance Abuse
    - Zero Tolerance, Consider EAP
  - Monitored or Limited Inventory
    - Inventory Logs
  - Data Back-up
  - Contingency Plan
    - Use All Hazards Approach
  - Responding Agencies
    - Plan with LEPC
    - On-Site Training with Responders
    - Test Plan in Segments
  - Preventive Maintenance
  - Cleaning Staff or Contractor
    - Continuous Training
    - Continuous Monitoring

Chapter 4

- **Site Specific Security Factors**
  - Image Portrayed by Company
    - Signage
    - Business Name
    - Products or Services
  - Significant Location or Surrounding Area
    - Federal
    - Historical
    - Large Population
  - Political in Nature
    - Social Agenda
    - Religious
    - Protectionist Affiliation
  - Chemicals or equipment
  - Location, Age and Type of Building
  - Hours of Operation

- Organize a "Neighborhood Business Watch"

INTRODUCTION

We all need to see Homeland Security as a personal issue. This is because decisions that may appear to be insignificant individually will collectively achieve our overall goal of national security. Owners and employees of small businesses can take actions or make decisions that unintentionally provide aid to the people trying to harm this country. The burden we assume as Small Business Development Center (SBDC) Counselor is making the subject real and meaningful to the entire range of small business clients and have them see, understand and act on the areas that fit their company.

This workbook is a resource for SBDC counselors and trainers to have real information about Homeland Security as it applies to our clients. We are using the word **Tools** in our title to help the reader visualize the act of building or repairing. Small businesses with our help must build something that doesn't yet exist or repair existing systems that don't function as needed. SBDC counselors can show clients that their security choices affect more than just their building and property. Surveys show that most small businesses are installing software and other devices to combat the most common security problems. It is true that there are many people spending time looking for weaknesses that can be exploited, but we know that is the way it has always been. Today we have to fortify our computer systems as well as our windows and doors. We have always had to watch for suspicious characters, but now some may be doing research or preparation for terrorist acts.

Many small business owners have questions, e.g., how is my small company going to have any effect on Homeland Security? What kind of strategic value to the security of our country could a small business have? The town or city in which our business is located is small or not a likely target of any terrorist group? We are in a big city, but isn't our company too small and anonymous to be a target?

We need to know and accept the fact that our country is not separate and invulnerable. We are part of the world and the world economy. The people and businesses of the United States will participate in the events of the world by choice or by economic and cultural forces that we can help shape, but cannot stop or ignore.

The information and the checklists in this book emphasize that homeland security is not just dealing with the stereotype of a terrorist. We are also dealing with domestic terrorists, drug-dealers, thieves, vandals and even possibly employees. Threats or attacks can be by people from any religion, race, sex or country. Attacks don't have to come from someone physically being on your premises or within a certain distance. Attacks can be launched from any place in the world and it may not be your business that is harmed, but your business may be affected only as part of an attack on any other business anywhere.

OVERVIEW

Most people don't realize that terrorist organizations finance much of their operations from drugs, either from selling drugs wholesale or in direct trades of drugs for weapons. Most of us acknowledge the personal damage suffered by drug-users and often their families, but the use of drugs by the people living in the United States and Europe has the potential to be even more destructive than we currently recognize. Retail or street level dealers may have no idea that they are buying from terrorists or their intermediaries, but the sales go on and the demand for drugs and the money generated makes its way back to the people we are fighting.

Many times the motive behind theft, whether by criminals or employees is to sell the stolen goods or information for money to buy drugs. The information stolen most often is intellectual property or financial records that can be used to steal more money.

The thread that ties this to the SBDC network is that most drug users, approximately 75%, are employed and nearly all of them are employed by a small business. This is not by accident as drug users are aware of which companies are least likely to detect them.

We, as counselors are here to pass along this information and keep small businesses educated of the need for criminal background checks and a solid random drug-testing program.

Another area of emphasis is how to avoid becoming a victim of computer crime. This is much more difficult to identify than in the past, because there are many more ways for the computers of a small business to be used by criminals. The potential methods range from old-fashioned theft of the equipment, to breaking into the computer system from another part of the world and using the system, for example, as part of a network to sell pornography. The computer system can be used without doing damage to the computer and the owner has no knowledge it is being used. Don't forget that it is still more likely for your computer security to be breached by employees or other people with inside access than from any other source.

Keeping your computer system protected from hackers is now essential to business continuity. This requires at a minimum the use of high quality firewall, intrusion detection and probably intrusion prevention software, so you can keep most people out and know when someone is trying to get in. Even if you only have one computer and you are using at least a DSL or Cable broadband connection to use the Internet, including e-mail, you are vulnerable.

Without taking precautions, you may be allowing someone to use your computers to attack other companies' systems. Hackers can insert programs into your system that will work on their command. They may be recording keystrokes used on your system looking for passwords or credit card information. They may use your system to get them into another system. Either way this can lead to theft of financial information, intellectual property, identity theft, damage to business web sites, damage to the Internet, and even the World Wide Web infrastructure (all of which have Homeland Security consequences).

We are trying to correlate common security issues, with which most small businesses should be familiar to the responsibility small business has in providing for Homeland Security. Criminal actions that previously would have an impact only on a specific place of business and possibly some of their customers or employees, can now impact the country.

We still think in terms of the local drug dealer and the effect on our neighborhoods, children, property values, customers and our places of business. This is not a bad thing because that is where the battle has to be won. It has not yet become a shared vision to equate the purchase of drugs locally with providing money for the purchase of weapons or terrorist training that will be used against our country and citizens.

In the last few years there have been thousands of successful viruses, worms, denial of service and other attacks on our computer systems. Some have had minor success and others have had a major impact. The financial losses, though not widely publicized, have been reported to be from the hundreds of millions of dollars to potentially more than a billion. This has all been done, as far as any one knows, by thieves and hackers only. Some hackers may have political motives, but it doesn't appear that we have yet had the big concentrated attack by a major political enemy or terrorist group trying to bring down the economy of the United States. To some degree this is still a form of protecting our neighborhood, whether the hoodlums are located all over the world striking electronically or they are physically working in the business facility doing their damage on-site.

A large percentage of small and mid-sized businesses report that they have responded to possible computer attacks by having firewalls, virus protection software and in many cases intrusion detection software installed. There are still far too many companies that have unprotected computer systems. In some ways leaving your computers vulnerable might be described as providing ammunition to the enemy. The companies that have installed software, to continue to be effective, must be active in keeping up with changes in protection both upgrading the current system and installing new defenses against constantly changing methods of assault.

Because we have always heard and seen Homeland Security treated as a worldwide issue, having the appearance of being bigger than any individual or small business, it is difficult to focus on the actions we should take locally.

Security for your business should be built in layers, it should be appropriate for the location and type of business and it should be in the form of a written plan. There is no need to let the complexity of Homeland Security stop anyone from implementing the simple security measures their business should have anyway. If a business' computer system is vulnerable, then it may be exploited by a kid down the block or by an organized crime ring in another country, because they both have access to the same tools to cause harm to your company, your customers and to the country.

GOALS

Vulnerability Assessment

The book **Homeland Security Tools for Small Business** is based on an outline designed to capture an overall plan with specific actions that can be chosen if they fit the business being assessed. The outline is provided in the section titled **CONTENTS** located at the beginning of the book. This organized list of headings and sub-headings is the place to start a **Vulnerability Assessment**. Look at the outline and you will see specific sections that you know immediately apply to your business. You will probably recognize other sections immediately as not being relevant to your company. It is a good idea to use other people to help determine what areas should be included. You might want to use someone that is not connected to the business to get a fresh perspective. You should consider thinking on a larger scale than most small businesses see themselves, because in today's world others have the ability to damage a business from a great distance and yet have no personal knowledge of the company or the owners. Read the individual sub-headings and refine the outline for your assessment. Then describe in as much detail as you can each area that is vulnerable, what the vulnerability is, what effect that can have on the company and what you can do to provide the necessary security. This information is used to develop action items, budgets and timelines or what we call "The Plan".

The Plan

The Plan can be called a Security Plan, a Risk Management Plan, a Crisis Management Plan, the name is not as important as having it in written form. The Plan also needs to be posted in a convenient place and employees need to be trained regularly on implementation.

An SBDC client base typically will cover a very large range of business types and sizes. Each small business will have many variables that are unique to that company in that location. For example if four hypothetical businesses were identical in size and services provided and were only judged on location then the following would factor into the Vulnerability Assessment:

1. Company One is located in a high-rise office building that also has the offices of a major oil company and a large banking facility.

2. Company Two is located in a small office complex, one block from the entrance to a hospital that serves the entire county.

3. Company Three is located in a rural area, but about one-quarter mile away is a manufacturer that has an eight thousand gallon tank of ammonia.

4. Company Four is located in a small suburban community and has no known chemical storage, special landmarks, military presence, medical facilities or controversial companies within one mile.

These businesses could be a one-person operation or a 300-employee facility and in two of the examples it could even be a home-based business. The point here is that each of these businesses has to assess the location within which it operates and identify any vulnerability presented by that location. Then they each determine the potential consequences of the vulnerability and the potential likelihood of any particular incident occurring. Depending on the result of the assessment a priority is assigned and a method for handling the situation is written into The Plan.

Hardening The Small Business - Layers Of Protection

Hardening the target is common security terminology that simply means making the target more difficult to attack. This can be one action, such as putting the entire company under a 20-foot concrete bunker. This may have its place, but wouldn't typically be the best strategy.

We prefer to discuss Layers of Protection. This means using many smaller actions that taken together provide adequate security for the business being protected. Depending on the reasons or the skills of someone attempting to enter your business, multiple barriers may cause them to give up or slow them down so they are caught before they can infiltrate and cause damage or carry out any other plans.

Each business has unique risks that the vulnerability assessment will define and the security plan will take into account. Manufacturing or service industry, office building, strip mall, warehouse or even home-based businesses all have security needs. The government is not going to tell you what to do. What you need to do and what you will do will be determined by you and the examination of your specific risks, threat potential or likelihood and resources available.

This workbook contains more than 450 questions that we thought were good examples for each of the subjects in the outline. When you work on a vulnerability assessment use any of the questions we included, but please try to think of more. Find questions that apply to your business to capture scenarios that are not always obvious. We want this book to provide small business owners with answers to questions such as:

Checklist

- ❒ 1. What is Homeland Security when applied to Small Business?
- ❒ 2. How does Homeland Security apply to small businesses?
- ❒ 3. What does the government require?
- ❒ 4. What do I need to do for my business and my employees?
- ❒ 5. How do I keep from wasting money that I don't have anyway?
- ❒ 6. Is there a workbook with checklists that can be used as tools?
- ❒ 7. Are there any ideas and information about security operations for small business that increases the safety of the business, its employees, and of our nation?

Chapter 1

Areas of Concern: Outer Layers (Facility Perimeter)

The outer perimeter is considered the first layer of security. You want the business to be protected and generally you want to stop unauthorized entry at this point. Don't forget to have other layers that will help delay or discourage possible entry. The idea is to cause the person to give up or be caught before they can complete their attempted entry.

Checklist

- ❒ 1. Is your business freestanding, in a strip mall or a multi-story building?
- ❒ 2. Does the building have any setback from the street or parking?
- ❒ 3. Is there access to the property other than from the street?
- ❒ 4. Is there a landscaped or open buffer area around the building?
- ❒ 5. If there is landscaping, can it be used as a hiding place?
- ❒ 6. Is the property enclosed by fencing with or without barbwire?
- ❒ 7. Is the area around your office public space or private?
- ❒ 8. Is the outside of your office set up to prevent unauthorized entry?
- ❒ 9. Is there a perimeter system in place to stop burglary, theft or vandalism?
- ❒ 10. Is the outer layer of security a deterrent to bomb threats or terrorist acts?
- ❒ 11. Is your company located in an urban area, a small town, or a rural area?

Intrusion Prevention

Fences

When a fence is used it should be considered the first layer of security. This also applies to the gates and doors with locks. Gates and locks may lead a person to find another way through the fence and the fence can be vulnerable if a person trying to break in has a place to hide. If your security system depends on a fence then your assessment should highlight the main weaknesses and address them. Security personnel must maintain the integrity of the fence and the ground under it by not allowing fasteners to deteriorate, holes in the fence, holes under the fence, bushes, trees, containers, tanks or trucks or anything that can provide a place to hide. Eliminating places to hide should discourage a person from crawling under, climbing over or cutting through the wire, because they might be seen by anyone looking.

Some businesses want a fence to be the only defense so they use a tall fence, with lots of razor wire. This may be effective, but some experts believe that this can lead professionals to wonder what needs so much protection behind such a fence and they may break in to find out.

Checklist

- ❒ 1. Is part or all of your property fenced?
- ❒ 2. Are gates and locks incorporated with the fence?
- ❒ 3. Are keys accounted for and limited?
- ❒ 4. Is the physical integrity of the fence checked regularly?
- ❒ 5. Is the ground under the fence checked regularly for possible breaches?
- ❒ 6. Are the grounds maintained for best visibility?
- ❒ 7. Are there more layers of security beyond the fence?
- ❒ 8. Is the fence appropriate for the facility and the security needed?

Signs

Signs are often overlooked as an effective security measure. Alerting criminals to specific precautions taken may convince them to move to a place that is easier. Many times only the sign is needed to prevent the crime.

Security policies that are posted need to be in effect at all times to work. Non-enforcement of procedures will be noticed and may be used against the company by employees, ex-employees, friends or accomplices of employees, temporary employees and/or independent contractors.

Checklist

- ❐ 1. Do you have signs posted informing of your security measures and procedures? (i.e., monitored surveillance, computer password protection, visitor identification)
- ❐ 2. Are signs inspected for vandalism, deterioration or other damage?
- ❐ 3. Are posted policies and procedures maintained consistently?

Security Lighting

Proper and adequate lighting generally provides a major component of company security. Surveillance is very difficult without proper lighting. Lights should be difficult to reach and protected from damage. To maintain security burned out or damaged lights must be fixed immediately. Often would-be intruders will create dark areas by disabling lighting, providing cover for unwanted and potentially damaging activities.

Checklist

- ❐ 1. Do you have security lights?
- ❐ 2. Are lights placed by design to eliminate dark areas and help visibility?
- ❐ 3. Are lights installed so they are not easily reached or damaged?
- ❐ 4. Is all lighting inspected continuously for removal or damage?
- ❐ 5. Is maintenance prepared to repair or replace immediately?

Gates and Turnstiles

Do you need to control access to your business or is it open to the public without any barriers? If people walk directly into the business and are greeted by a receptionist, the door should sound an alert that someone has entered. The desk should be situated so the visitor is not between the receptionist and an escape route. As the need for security is increased, the door between the reception area and the rest of the building can be locked manually or electronically and can be opened by the receptionist or security guard. Reception area windows can be shatter-resistant, shatterproof or bulletproof. Gates and turnstiles can be simple or complex in operation. They can be unmonitored or monitored by an attendant or remote surveillance and can be opened remotely, with an electronic ID card or even using a biometric system.

Checklist

- ❑ 1. Do you have a need to control access to the business?
- ❑ 2. Is the area designed to be safe for the receptionist or security guard?
- ❑ 3. Does the door sound an alert when opened?
- ❑ 4. Do you control access to areas of your facility with gates or turnstiles?
- ❑ 5. Is there an emergency back-up plan in the event any or all of your control devices fail?
- ❑ 6. Does someone regularly verify that all the equipment is working properly?

Setbacks and Clear Zones

Setbacks have been used for many years as a zoning requirement mainly for aesthetics. Setbacks can be effective in traffic control when combined with proper landscaping including vehicle barriers.

Vehicles and people can be guided to be where you want them and setbacks at 50 to 80 feet can be part of a blast resistant building design. This much space may make intrusion detection easier depending on the landscaping.

Home-based businesses, businesses with parking on the street, businesses located in a strip mall like setting or businesses located in an office building may have no options. Someone other than the business owner determines parking and setback from the street.

Blast-resistant windows, which reduce many injuries from an explosion also provide protection against break-ins and smash and grab attempts.

Checklist

- ❒ 1. Can you determine how the building is located on the property?
- ❒ 2. Can you design parking to be 50 feet away from the building?
- ❒ 3. Is the space around your business location public or private?
- ❒ 4. Can part of the setback be open perimeter inside the business?
- ❒ 5. Have blast-resistant windows been installed?

Barriers, Posts, Fountains, Trenches and Other Landscaping

Visibility, need and the budget available all help determine whether building security design is strictly functional, is incorporated into some of the landscape elements or if the landscaping itself becomes the security.

Today you may see shrubbery that has concrete and steel posts incorporated and painted to match. Concrete and steel barriers are now being shaped and painted to resemble large fruits and vegetables for at least one grocery chain and one restaurant chain. These are located to stop a vehicle from driving through a wall of the building and are also attractive and relevant to the business.

Trees, fountains, planters, reinforced benches, and street lamps are all being strategically placed to block or guide movement through an area and are attractive too.

Checklist

- ❑ 1. Does your business have an ATM or product near a wall?
- ❑ 2. Could smash and grab be a method used on your location?
- ❑ 3. Could your business benefit from less obvious security measures?
- ❑ 4. Will you be adding landscaping or landscape elements?
- ❑ 5. Do you have a setback area that needs to be used more effectively?

Control Access and Approach

Walk in the front door of most small businesses, it is likely that there will be a guest book to sign. This is a very simple system used to manage and verify visitors. Depending on the business this method may be adequate. It is common knowledge some visitors use this book to see who the company might be buying from, selling to or who may have visited. A person with a reason could use this information to gain access by pretending to represent a company in the book. If there is a need for stricter security, require an appointment and a picture identification that is copied and kept. In every case call the visitor's employer, verify the identification and that the visitor is supposed to be at your location.

If access requires additional layers of management many new systems are available. Security guards are often used, but high tech controls are beginning to be introduced. For example there are several ways to use thumb, finger or palm prints to provide identification. Eye scans are starting to show up in a few places.

Be very careful when choosing the newer technology because some equipment has been refined and works very well but not all equipment is foolproof. Some equipment for all existing identification methods has been fooled. Sometimes it is as easy as using a picture of the fingerprint or an eye, a method usually known as spoofing.

Checklist

- ❑ 1. Do you use a guest book or individual sign-in forms?
- ❑ 2. Do you require visits by appointment only?
- ❑ 3. Do you verify all identification and appointments?
- ❑ 4. Do you require more sophisticated access security?
- ❑ 5. Do you have a back-up system in case of power failure?
- ❑ 6. Do you ever mystery shop your access security?

Intrusion Detection

Motion and sound detectors hooked to the local police or a security monitoring company is basic for many small businesses. Lighting adds more protection, sometimes with security cameras for additional defense. The cameras can be monitored on-site or from a remote location. Today up to 16 separate cameras can be monitored from any location that is convenient to you. Using the Internet, monitoring can be done from any computer set up properly, wireless laptops, PDAs, and even cell phones. Usually all of the functions of pan, tilt and zoom (PTZ) cameras can be operated over the Internet.

Checklist

- ❑ 1. Are motion and sound detectors tested regularly?
- ❑ 2. Do you have enough properly installed lighting?
- ❑ 3. Is response time to an alarm fast enough?
- ❑ 4. Do you have enough cameras in the right locations?
- ❑ 5. Are the cameras monitored sufficiently?
- ❑ 6. Is the security system tested regularly?
- ❑ 7. Do you have a back-up plan if the security system fails?

Security Guards Posted and/or Site Patrols

If your small business has or decides to have on-site security guards don't use just a low bid to choose the company. Small security firms will often have very low pay, very long hours, high turnover and few if any benefits. It is not unusual for the employees to have 1 or 2 other jobs and get by on very little sleep. No federal requirements govern private security companies, who they hire and what training they must have. Require that the guards used at your facility be fully and properly trained, licensed, and subject to federal background checks. Criminals do get hired as security guards; sometimes background checks aren't done at all or the check is done at the state level and misses a criminal record in another state. It is easy to see that determined dangerous people could outsmart untrained guards or could become one of the guards and work from the inside.

Checklist

- ❑ 1. Do you have a detailed background check on the security company?
- ❑ 2. Do you know wage rates, hours and benefits for the employees?
- ❑ 3. Do you have records of education, training, licenses and criminal history?
- ❑ 4. Do you have a method to vary the site patrol times and route?
- ❑ 5. Do you have a method to monitor the security employees?
- ❑ 6. Do you ever mystery shop your security system?
- ❑ 7. Do you have a written plan in the event of system failure?

Limiting Damage—Potential Targets

Potential targets for damage are not limited to the building or trying to get into the building. The goal may be to damage something outside that affects the operation. Try to think of anything that can be broken into, used, attacked, damaged or stolen, thereby compromising the security of a business.

We tried to identify parts of an operation that would normally be kept or used outside the building or things that enter the building from the outside. Our list, which is not exhaustive, includes:

- ❒ Other Buildings
- ❒ Storage Tanks
- ❒ Process Equipment
- ❒ Production Equipment
- ❒ Boilers
- ❒ Power Supply
- ❒ Operational Control Systems
- ❒ Back-Up Power Supply
- ❒ Water Supply
- ❒ Wastewater Treatment
- ❒ Air Vents (Intake and Exhaust)
- ❒ Communications Equipment
- ❒ Heavy Equipment and Forklifts
- ❒ Trucks and Trailers
- ❒ Rail Stock
- ❒ Docks and Piers
- ❒ Raw Materials
- ❒ Hazardous Materials and Waste
- ❒ Finished Goods

All businesses, even very small and home-based have at least some parts of this list that will be in a vulnerability assessment. If someone damaged the electrical or phone lines coming into your office, how much business would you be able to do? Have you ever considered what is vulnerable, how is it accessible and how it can be protected?

Buildings

The building where your business is located or any out buildings where you might have storage or process or production equipment are vulnerable to damage. Someone may want to enter for what is inside or they may want to stop production or cause other financial hardship. A second possibility is that your business is located near or next to another facility that is a target and you suffer collateral damage.

Checklist

- ❑ 1. Is there cash, valuable materials or information inside the building(s)?
- ❑ 2. Is your business co-located with or near any controversial businesses?
- ❑ 3. Are you near any military, landmark, political or government buildings?
- ❑ 4. Do you have steel doors and high quality locks?
- ❑ 5. Are the walls concrete, stucco, steel or other strong materials?
- ❑ 6. Do you have windows that resist breaking, shattering, bullets or blasts?

Storage tanks

Businesses with outside storage tanks are known to attract attention. Depending on the contents of the tanks, vandals may decide to do damage for fun. There may be criminals that want the material to sell for money or for manufacturing of drugs. If the chemical is dangerous or toxic enough, terrorists may want to cause a chemical release that might cause damage over a large or heavily populated area. They may also want to steal the chemicals to make weapons.

Checklist

- ❑ 1. Do you have layers of security to protect outside tanks?
- ❑ 2. Do you have separate fences around tanks?
- ❑ 3. Do you have a containment system around the tank(s)?
- ❑ 4. Do you have a liquid detection alarm system in place?
- ❑ 5. Do you have flow control valves in place (see Chapter 2 for details)?
- ❑ 6. Do you have video surveillance or regular security patrols?
- ❑ 7. Are your security systems all checked regularly for failure?
- ❑ 8. Are the tanks checked regularly for structural integrity?
- ❑ 9. Do you have a written emergency plan for chemical tanks?

Process Equipment / Production Equipment / Boilers / Power Supply

Equipment located outside or in out buildings may be subject to damage from vandals or disgruntled employees. If anything valuable can be removed then theft can become a possibility. Boilers can be damaged to prevent use or they can be used to cause an explosion. Power Supplies can be damaged to stop operations or can be used to start a fire. Boilers and power supplies are dangerous in general, a professional could probably cause problems while amateurs and vandals could easily cause severe injury to themselves.

Checklist

- ❑ 1. Have you installed layers of protection?
- ❑ 2. Are equipment, boilers and power supplies inside a building or fence?
- ❑ 3. Are locks, doors and windows resistant to break-ins?
- ❑ 4. Are forklifts stored or disabled so they can't be used for break-ins?
- ❑ 5. Are equipment, boiler and power supply controls secured or disabled?
- ❑ 6. Do you have video surveillance or security checks?
- ❑ 7. Are operation or tampering alarms in place?
- ❑ 8. Do you have a back up plan or replacements available?
- ❑ 9. Do you have a written emergency plan in case of security failure?

Operational Control Systems

Using electronic controls to manage equipment through the Internet or through an Intranet system has allowed for less expensive, more productive use of operations personnel. One person can monitor and modify controls from a remote location. These controls will usually be located in the main computer system with access given only by password or possibly biometric identification. Because this section is about outside or perimeter security we have to expect the controls are being exploited by hackers who break into the system to cause incidents, accidents, minor or serious damage. Valves can be opened or closed; temperature sensors can have the settings changed, programs can be altered to affect quality of products and many other problems.

Monitoring of Internet activity has discovered millions of continuous attempts to find access into power systems, water and wastewater systems, chemical storage and process systems all across the United States and European countries too.

Checklist

- ❑ 1. Is firewall, intrusion detection and intrusion prevention software installed?
- ❑ 2. Do you require passwords to be complex and changed often?
- ❑ 3. Do you have video surveillance or security checks of equipment controls?
- ❑ 4. Do you have monitor alarms installed to report dangerous levels?
- ❑ 5. Can you lock out electronic controls when not in operation?
- ❑ 6. Are controls and security checked frequently for failure?
- ❑ 7. Do you have a back up plan if equipment or controls are damaged?
- ❑ 8. Do you have a written emergency plan in case of accidents?

Back-Up Power Supply

Diesel powered generators come in a variety of sizes that will provide back-up power for a home-based business, a small office space or building or very large operations.

Regular testing (daily or weekly) along with proper layers of protection should assure the power will be there if it is needed. If you need to provide power even for a short time to critical equipment or areas then regular and up to date training will be needed too. Owners, responsible employees and their back-ups should be trained in operating and shut down procedures as well as operation and troubleshooting of the back-up power system or equipment.

Because generators and the supply of diesel fuel will probably be located outside, additional security will be necessary to keep anyone from tampering, damaging or stealing. When practical, emergency equipment should be locked inside an out-building. If the equipment is too large and/or if there is fuel storage in a tank a secondary fence with a heavily locked gate might be a second choice to protect emergency equipment.

Checklist

- ❑ 1. Do you have a back up power supply system in place?
- ❑ 2. Do you have a regular testing and maintenance procedure?
- ❑ 3. Do you have layers of security for the equipment and fuel storage?
- ❑ 4. Do you have a written back up plan if the back up power fails?

Water Supply

This may be considered an unusual issue for most businesses. Your water supply is probably provided by the city and should be very difficult to reach at your facility. This is included because it is supplied to the business from the outside and losing water can easily stop production.

Consider the effect on your business if someone breaks a main water line, damages the water treatment plant or contaminates the water supply. Normal water supplies could be shut off to your business from a couple of days up to a few months. This would be a powerful weapon to disrupt the United States economy.

Checklist

- ❑ 1. Do you have loss of water supply in your vulnerability assessment?
- ❑ 2. Do you need water as part of your operation?
- ❑ 3. Do you have access to an alternative source or water?
- ❑ 4. Do you have cost projections for alternative water sources?
- ❑ 5. Do you have an alternate operations location where there is water?

Wastewater Treatment

A small business that does manufacturing or some service that requires a wastewater treatment plant would want to include this in a vulnerability assessment. Most chemicals used to treat wastewater can cause serious illnesses, injuries, and even death.

Access to these chemicals and access and the wastewater treatment facility need to be secured from theft and or release, accidentally or on purpose.

If a person were to damage the wastewater treatment facility probably production would have to stop until repairs could be made and an inspection given by a city, county or state official.

Checklist

- ❑ 1. Are the treatment facilities and chemicals secured by a building or fence?
- ❑ 2. Is access to this facility strictly controlled?
- ❑ 3. Has any equipment been identified for temporary or emergency use?
- ❑ 4. Are there any alternatives allowing operation without waste treatment?
- ❑ 5. Do you have a plan and an agreement for emergency repairs?
- ❑ 6. Do you have financial projections that include stopped production?

Air Vents (Intake and Exhaust)

The Outdoor Air Intakes for the Air Handling Units (AHU) of the Heating Ventilating and Air Conditioning equipment are important to include in a vulnerability assessment. Specifically the location and angle of the intakes will affect the potential for contamination from Chemical, Biological, or Radiological agents (CBR). CBR agents can be present from incidents such as an accidental hazardous chemical spill outside or near your business. CBRs can also be deliberately released inside or outside your building. The Outdoor Air Intakes might be needed to exhaust these agents from inside the building or provide an adequate seal to keep the agents outside.

The best design for outdoor air intakes is to be flush and high up on the building making access difficult, if not impossible. There are various modifications you can make to your system if needed. Outdoor Air Intakes that are at or near ground level or at or near roof level can be covered with an extension that is approximately 12 feet up and on a 45 degree angle at the top.

Checklist

- ❑ 1. Do you know where all Outdoor Air Intakes are located?
- ❑ 2. Is access to those Intakes secure and limited?
- ❑ 3. Do you know how well the building and ventilation system can be sealed?
- ❑ 4. Do you have the ability to exhaust only?
- ❑ 5. Do you have re-circulation capabilities?
- ❑ 6. Do you have a written shelter-in-place plan?
- ❑ 7. Do you have a written evacuation plan that considers exhaust?
- ❑ 8. Have local emergency personnel toured the building?
- ❑ 9. Have written plans and drawings been given to police and fire officials?
- ❑ 10. Have employees been trained and practiced emergency plans?

Communications Equipment:

Keeping communication lines for phones and computers and other equipment secure is essential to any business. Access to the communications equipment and points where lines enter and leave the business should be limited and monitored. These areas should be considered vulnerable and at risk; they should be identified, assessed and if possible hardened using safe routing or barriers. Small business communications systems may be easier to tap into or to hijack and use for malicious purposes.

Checklist

- ❑ 1. Is communication equipment and lines entering and leaving secured?
- ❑ 2. Is access to outside equipment and lines limited and monitored?
- ❑ 3. Have you installed physical barriers to secure outside communications?
- ❑ 4. Is outside communications equipment inspected and tested?
- ❑ 5. Do you have redundant or back up communications equipment?
- ❑ 6. Do you have a written plan for operations during communications failure?

Heavy Equipment and Forklifts

Heavy equipment and forklifts should be stored and locked inside a building or a fence whenever possible and should be disabled when not in use. These are layers of protection that help stop theft of the equipment or using the equipment to break into buildings.

Vandals often break into a business to joy ride on big equipment and typically damage the equipment and other property. Criminals may steal the equipment and use it to break down overhead doors, fences and office doors, which allow them access to steal other valuable equipment or information.

Checklist

- ❑ 1. Is access to heavy equipment or forklifts limited and secure?
- ❑ 2. Do you have a procedure to disable this equipment when not in use?
- ❑ 3. Are LPG tanks stored securely in a locked area with controlled access?
- ❑ 4. Does the vulnerability assessment consider heavy equipment or forklifts?
- ❑ 5. Do you have a written plan that covers potential theft or damage?

Trucks and Trailers / Rail Stock / Docks and Piers

Outdoor storage always provides temptation for attempted theft of the contents. Shipping equipment such as trailers, railcars and containers used for storage may be easier to break into than a building. Sometimes the thieves want the contents and sometimes they only want something of value to sell. The vulnerability assessment should identify any materials that can be used in the manufacture of drugs, chemical weapons, biological weapons or explosives. These items should receive very high priority for security. Rail stock and shipping containers are not often stolen from storage, but in the case of trucks and trailers they may be stolen even if empty. Trucks and trailers can be used for moving materials or to sell for financing other activities. Do not leave trucks and trailers parked near fences or gates where they can hide breaking and entering. When security is minimal or problematic it is a good practice to unload all shipping equipment that arrives late and not load shipping equipment the night before for shipment the next day.

It is very important to consider that any shipping equipment can be used as a weapon or a weapon delivery system without the knowledge of the owner or operator, in a similar manner as the airliners were used on September 11, 2001. The different possibilities are nearly limitless. For example, this could be duplicated using tractor/trailers making deliveries to buildings that are designated as targets or near designated targets.

A person using radio-controlled detonation would only need a container to be driven through a target area to allow a serious bomb blast to be delivered. Small businesses are just as likely if not more likely to be used in such an attack because security efforts at small companies may be more easily defeated.

Checklist

- ❑ 1. Do you ever use trailers, railcars or shipping containers for storage?
- ❑ 2. Can materials stored be used to make drugs or weapons?
- ❑ 3. Is any shipping equipment stored outside the perimeter security?
- ❑ 4. Are received shipments left overnight for unloading?
- ❑ 5. Are early shipments loaded the day before?
- ❑ 6. Is shipping equipment kept locked when empty and not in use?
- ❑ 7. Is all shipping equipment completely inspected regularly?
- ❑ 8. Do you have a written plan for dealing with theft, sabotage or vandalism?

Raw Materials / Hazardous Materials and Waste / Finished Goods

Small businesses may use outdoor storage for raw materials, finished goods or waste materials because of space limitations. These materials need to be assessed for potential misuse or value as stolen property. Raw materials and finished products would probably receive very good security making access difficult. Small business owners are required to protect hazardous waste from contaminating their property, but that may not include the possibility of it being stolen. Hazardous waste containing one or more of many different types of chemicals could be used to add damage from an explosion. A chemical dirty bomb could be made more powerful. Flammable wastes may provide fuel for a hotter faster burning fire. Certain waste might put dangerous chemicals into the air that could cause more casualties, require special equipment to approach and significantly slow down rescue, containment and cleanup.

Checklist

- ❑ 1. Do you store any materials outside the building but inside the perimeter?
- ❑ 2. Do you provide additional layers of protection for outside storage?
- ❑ 3. Do you protect hazardous waste from theft or vandalism?
- ❑ 4. Do you keep a daily or weekly inventory of all materials stored outside?
- ❑ 5. Have you provided a chemical list to Police, Fire and LEPC personnel?

Chapter 2

Areas of Concern - Inner Layers (Facility)

Home-based businesses, commercial office buildings, or manufacturing facilities all need policies and procedures that allows only authorized people to be in your place of business. Each topic discussed covers the problems they present from inside the business. Security risks on the inside can include employees, ex-employees, employee spouses/other friends, sales representatives, contractors, customers and computer hackers both inside the building and outside the building.

Checklist

- ❑ 1. Do you have layers of security for the inside of the business?
- ❑ 2. Do you have a plan that considers all potential security risks?
- ❑ 3. Do you have policies to protect physical, financial and intellectual property?

Unauthorized Entry

What policies do you use to prevent unauthorized inside entry? Locked doors that provide easy safe exit for employees in case of an emergency but no entry from the outside will provide a layer. Locked doors work if employees don't prop open the door or open the door for friends, family or previous employees. If policies are not being followed inexpensive video surveillance equipment can be purchased and used to record or enforce proper procedures for the entry of any person (employee or non-employee).

Checklist

- ❑ 1. Do you have layers of security beyond the doors and locks?
- ❑ 2. Do you have a written policy for opening doors into the facility?
- ❑ 3. Do you have a system for monitoring entry into the facility?
- ❑ 4. Do you have video surveillance or unannounced security checks?
- ❑ 5. Do you have a written plan in case there is failure of the security system?

Theft
Substance Abuse
Trade Secrets
Intellectual Property

Providing inside security for the four subtitles above are in many ways connected. Theft in a small business can cause serious financial problems. The list of items with value is longer than you might think including: raw materials, finished goods, waste materials, cash, checks, bank account information, credit card data, customer information, trade secrets and patent information. The thief or thieves can be anyone with access, authorized or not, such as an individual employee, a group of employees with or without outside help, it may be organized criminal activity and it may be by computer where a person never enters your property. Many times the loss in real or calculated dollars can also be increased by financial liability or law suits being added to the initial theft.

Theft in the workplace is often to support the purchase of drugs that may be used or resold or both. Sometimes the drugs are sold to other employees in the workplace.

Small business owners trying to understand their link to Homeland Security can find it here. Terrorism is funded with lots of cash, but much of it is raised through what we would consider small time criminal operations. On the international level drugs are traded directly for weapons. Individual terrorist cells working in the United States or in Europe raise cash by selling drugs to people that may be working for you. A second major source for cash and meeting daily needs is through identity theft.

Checklist

- ❒ 1. Do you do criminal background checks on new employees?
- ❒ 2. Do you have an operating, consistent random drug-test program?
- ❒ 3. Do you have an inventory or other controls to track physical items?
- ❒ 4. Do you have controls to protect information and intellectual property?
- ❒ 5. Do you have insurance protection against losses and loss liability?
- ❒ 6. Do you have a procedure to check internal controls for tampering?
- ❒ 7. Do you have a written emergency plan in case of business interruption?

Disgruntled Employee
Contractor actions
Workplace violence

What is a terrorist act? What we called vandalism in the past may be described as terrorism today. We are aware that some acts, though limited in scope, can still be terroristic in intent and result. It is possible for any business to be the target or receive collateral damage from actions of a person or persons unknown to you. But, it is still most likely a person or persons conducting an assault on your business would be disgruntled employees or former employees, contractors or employees of contractors, spouses, former spouses or other people with a personal relationship involving an employee.

These are all people who should be screened by your authorized entry procedures before being allowed to enter the facility. In many cases, if entry is allowed, the person or persons should be required to have accompanying supervision.

Checklist

- ❒ 1. Do you have a procedure to identify potentially volatile situations?
- ❒ 2. Do you have a procedure to deny entry of unauthorized people?
- ❒ 3. Do you have a procedure for managing authorized suspect persons?
- ❒ 4. Do you have a procedure to handle damaging or violent situations?
- ❒ 5. Do you ever mystery shop your security polices for these issues?
- ❒ 6. Do you have a written emergency plan if the procedures don't work?
- ❒ 7. Have you had police or emergency medical people in for a visit?
- ❒ 8. Do the police and fire department have a copy of your emergency plan?

Material Contamination
Equipment Damage
Production Stoppage
Sabotage
Terrorist Acts

Terroristic acts and Homeland Security do not apply to just one group or type of tactic. The main goal may be to cause some financial hardship to a company or several companies at once. The result may be contained within one facility or may help destabilize the economy of an area, a State, a region or the nation.

Whether your company is a manufacturer, provides services at a customer's location or all services are performed in your office, all of the sub-headings above can happen to your business. The quality of a product may be compromised, equipment damage or other acts of sabotage may stop production or the facility may be damaged or threatened. Employees may not be allowed to enter or may be afraid to enter the workplace.

All business security should be designed to cover these principle areas of operation. Materials can also be supplies, equipment can be office equipment, including computers, which can be damaged without entering the building and if you can't provide your services then production is effectively stopped.

Checklist

- ❐ 1. Are material or supplies kept in a protected location?
- ❐ 2. Is access to materials and supplies restricted?
- ❐ 3. Do you have an emergency plan to replace materials or supplies?
- ❐ 4. Are access restrictions and security used to protect equipment?
- ❐ 5. Do you have a plan for access to back-up equipment or production?
- ❐ 6. Do you test security measures regularly for gaps?
- ❐ 7. Do you have a written crisis management plan?

Intrusion Prevention

Once past the perimeter or outer layers of protection the next set of layers begin. Whether someone is invited into your business, have forced their way in or are entering through your computer systems there are many places and ways to slow them down or stop them from doing additional damage. Hardening the facility continues on into the offices themselves to provide stronger security.

Offices and People Flow Arranged for Visibility

It is considered a good practice to keep visitors visible to someone while they are inside the business. If an unaccompanied person is able to slip unnoticed into an office and access the computer, then many of the IT Security protections are already bypassed and damage or theft is much easier. Physical damage can also be done, possibly without detection.

Access to the emergency exits is important and may not always be connected to a fire or other catastrophic event. An employee may need to exit quickly due to a threatening person. Try to seat visitors so they don't block an employee's ability to leave if necessary. Two exits should be provided whenever possible, particularly in reception areas.

Checklist

- ❒ 1. Do you have an open office design plan?
- ❒ 2. Are there several unoccupied offices or cubicles?
- ❒ 3. Has a redesigned office set-up been reviewed?
- ❒ 4. Do you have an escort with a visitor at all times?
- ❒ 5. Are emergency exits easy to get to?

Visitors by Appointment with Sign-in and Escort

It is not uncommon to prohibit drop-in visitors. Every person must have an appointment and must be escorted by the person with whom the appointment is made. One additional touch of security is to have the name of the escort on the nametag worn by the visitor.

Checklist

- ❐ 1. Do you have a policy and procedure for approving and identifying visitors?
- ❐ 2. Do you have a procedure for visitor escorts during visits?
- ❐ 3. Do you have a policy to deny entry further into the office?
- ❐ 4. Do you have a list of people that are not allowed to enter?
- ❐ 5. Do you have a procedure for accepting sales samples through receiving?

Locks on all Gates and Doors

Specifically all outside doors need to have key only deadbolt locks with the serial numbers removed. These locks should be locked at all times to prevent unauthorized entry. Employee safety requires easy exit from the inside. Depending on the business and the location of the doors, some should have alarms or video surveillance.

Checklist

- ❐ 1. Do you have deadbolt locks without serial numbers installed?
- ❐ 2. Are serial numbers kept in a secure location?
- ❐ 3. Are keys limited, signed for and return required at exit interview?
- ❐ 4. Are locked doors easy to open from the inside during an emergency?
- ❐ 5. Are closed and locked doors checked regularly and enforced always?

Access Control System with Audit Trail

Some access control systems include an audit trail. A record is kept of each entry or exit from specific areas using cards or keypads with a personal code to identify the user. Sometimes matching the audit trail with video surveillance is used to determine if someone is using a card or code other than the person authorized.

Photo IDs become useful depending on the size of a company and how much security a small company needs. If you start using Photo IDs then use a policy to require standardized locations for display on the person. Photos should be updated frequently to account for changing appearances.

Regardless of whether the ID card has a photo it can have vital information about the employee including finger and/or thumbprint digitally encoded on a magnetic strip. Newer technology now includes Radio Frequency Identification (RFID) that can be read automatically as a person passes through a gate or doorway and can contain all of the necessary information to provide a security audit.

Businesses where security is ranked as a highest priority will likely use some version of biometric identification. This can be as simple as a thumbprint reader attached to a computer or a PDA and a thumbprint database of all employees for comparison and access control. These are in common use and the equipment can be bought inexpensively from many computer and security suppliers. These can also be used to replace passwords for access to computers and other equipment.

Checklist

- ❒ 1. Does your access control have audit capabilities, including manual lists?
- ❒ 2. Is the audit information stored and not analyzed?
- ❒ 3. Is the audit information analyzed for patterns and anomalies?
- ❒ 4. Are photo ID badges displayed uniformly?
- ❒ 5. Are coded entry points also watched with surveillance?

Video Surveillance

Video surveillance today should go through a computer server and be stored on a computer hard drive. Surveillance can be done from any location over the Internet where up to 16 cameras can be observed simultaneously. Any camera that can be panned, tilted or zoomed (PTZ) can be operated from the keyboard. Camera views can also be seen from Internet enabled PDAs and even cell phones.

Checklist

- ❒ 1. Is video surveillance recorded on a VHS recorder?
- ❒ 2. Is video surveillance recorded in digital format?
- ❒ 3. Can you monitor video surveillance through the Internet?
- ❒ 4. Does video surveillance include any covert cameras?
- ❒ 5. Is access to monitors limited and secure?

Vehicle Entry Permission System

If your small business has property available to provide a designed security system, consider that the vehicle entry system should be at least as secure as that for visitors. For example, parking areas should be 50 to 150 feet from the building. The vehicle and the person with it should have an appointment and should have means to identify themselves and any cargo. Visual inspection should be made each time regardless of how familiar your security has become with the vehicle or the person.

Checklist

- ❒ 1. Does vehicle entry security require identification?
- ❒ 2. Does the person have to wait for approval and an escort?
- ❒ 3. Are inspections made regardless of frequency or familiarity?

Receiving and Inspection Process

Small businesses need to treat the mailroom or receiving area with the same care as any other important part of the company. Begin with the hiring process; this job should be viewed as one where criminal activity can take place through shipping or mailing in or out of the company. Potential employees for this work should information checks that contain criminal history, work references that have been verified, mandatory drug tests, and any IRS required Form I-9 information. If the company security system includes surveillance cameras receiving is probably an area that needs to be watched. All Mail, Parcels, Raw Materials, Equipment, Supplies and Product Samples should be required to go through receiving to provide tracking information that may be needed for later identification.

When setting up the area to receive mail and other shipments try to achieve the following:

- Located near an entrance
- Separate ventilation/area that can be isolated
- Easily and thoroughly cleanable

On the following website is a copy of a poster that can be downloaded from the U. S. Postal Service at www.usps.gov. Some of the following are on the poster and other items are not but are recommended by the Postal Services as a way to potentially identify dangerous mail and packages:

- Excessive postage, particularly when using postage stamps.
- Address is poorly typed, handwritten, or has misspellings.
- Very large or odd shaped packages.
- Packages with excessive masking tape, strapping tape, or string.
- No return address or return address different from the postmark.
- Package has oily stains, crystallization on wrapper or strange odors.
- Packages that are discolored or appear to contain liquid.
- Packages containing electrical wire or tin foil.

If you suspect you have a letter or package that contains a bomb, chemical or biological agent then immediately do the following:

- Do not smell, touch, taste, shake or bump the letter or package.
- Immediately wash your hands with soap and water.
- Notify security and contact 911.
- Isolate the area, shut off the building HVAC and all fans
- Do not allow anyone other than professionals to enter the area.

Limiting Damage – Potential Targets

Someone has circumvented the intrusion prevention defenses you have implemented and now has access to the entire business. We have divided the business into specific areas, identified vulnerable parts and discussed layers of security for each one. The specific areas are (Plant and Equipment); (Chemicals and Chemical Storage Containers); (Communications and Computers); and (Personnel - Full-Time, Part-Time, Temporary and Contractors)

(Plant and Equipment)

Well Designed Barriers Against Vehicles

Inside barriers, though sometimes designed for appearance, are usually designed for function. Concrete posts, vertical or horizontal I-beams and galvanized steel railings when set properly into a concrete floor provide a significant obstacle to ramming through a wall or door.

A forklift is one of the vehicles that might be inside a facility and can be used as a tool to break through a wall or door inside a facility. Don't forget that as well as being used to ram or batter, the forklift can also pick up items and drop them onto or into something that someone wants to open.

Checklist

- ❒ 1. Have you identified vulnerable doors or walls that need more protection?
- ❒ 2. Are doors locked with adequate equipment?
- ❒ 3. Have barriers been installed for protection?
- ❒ 4. Are forklifts and other equipment secured or disabled?
- ❒ 5. Do the barriers cause any safety problem for the employees?

Blast Resistant Buildings or Structures

Reinforced walls and windows are now being improved by the use of Kevlar or a combination of Kevlar and a carbon-fiber coating that is beginning to have the ability to absorb bomb blasts.

The latest designs in blast-resistant windows are meant to give with the impact of the bomb blast. The glass is heat treated and has layers that include plastic laminates so the glass may break but will not be able to fly around injuring or killing people. The frames are new materials as well and work together with the glass as a system. The demand for these windows or a laminate treatment has increased dramatically.

Checklist

- ❒ 1. Do you have any rooms that contain very valuable materials or goods?
- ❒ 2. Would anyone want to stop production by your business?
- ❒ 3. Would anyone consider this kind of damage retaliatory?

Design Layout to Limit Accessibility

The more centrally located valuable, damaging or controversial parts of the operation are the further someone has to travel to reach them. The layers of protection should make the attempt as difficult as possible.

The entire business cannot be located all inside a fortified enclave. Designing the business to be efficient is the first priority, but if less valuable or vulnerable operations or materials can be located nearer the perimeter that may help.

The safety of employees must be a top priority when trying to provide security for different sectors of the business. Emergency exits should always be easy to reach and operate with nothing blocking or obscuring access.

Checklist

- ❒ 1. Was security of the company operations part of the business design?
- ❒ 2. Can the business design be rearranged for security and be efficient?
- ❒ 3. Have you done a detailed vulnerability assessment to find gaps?

(Chemicals and Chemical Storage Containers)

Chemicals and chemical storage containers can be very attractive targets for terrorists and vandals. A person may cause death, injury, or environmental damage relatively quickly by releasing hazardous or toxic chemicals into the air or water or by setting fires or explosions.

Utilizing the "layers of protection" strategy, your first objective should be to make chemicals and system control mechanisms inaccessible to unauthorized persons. The next layer consists of control measures installed in and around the containers and lines. Following are some devices and strategies for securing stored chemicals:

Valves and Pumps Inside Buildings or Fences

A minimum layer of protection for control mechanisms and chemical storage would at least include enclosing with high security fencing and locks. Chemicals and controls that are contained in a locked building will protect the containers from the elements while making it more difficult for would-be vandals, but adequate ventilation is essential to prevent fume build-up.

Checklist

- ❒ 1. Are chemical storage area and controls secured with security fencing?
- ❒ 2. Are chemicals and controls in a lockable, well-ventilated structure?
- ❒ 3. Is video surveillance possible if chemicals and/or controls are outside?

Excess Flow Check Valves

Excess flow check valves (EFCV) protect against spillage in the event a downstream line ruptures, either accidentally or due to tampering. The valve closes the line when it senses a flow rate that exceeds a pre-set maximum.

Checklist

- ❐ 1. Are EFCV used in lines flowing into and out of pressure tanks?
- ❐ 2. Is valve operation tested routinely?
- ❐ 3. Are EFCV repaired or replaced as needed?
- ❐ 4. Do designated uses account for EFCV design limitations?
- ❐ 5. Are EFCV in railroad tank cars used only to prevent leaks during transit?
- ❐ 6. Are all personnel trained in causes of EFCV failure?
- ❐ 7. Is upstream pressure too low to produce excess flow?
- ❐ 8. Do downstream restrictions prevent excess flow?
- ❐ 9. Could a break in a flow line be too small to create excess flow?
- ❐ 10. Is there foreign material in the valve that prevents it from closing?
- ❐ 11. Has someone tampered with the EFCV, attempting to increase flow?
- ❐ 12. Is there damage to the EFCV due to prolonged hammering?

Overfill Protection

Overfill protection is designed to prevent spills by slowing and then stopping the flow of product before the tank overfills. The three most commonly used types of overfill protection are: automatic shutoff devices, overfill alarms, and ball float valves.

Spill protection for Underground Storage Tanks (UST) utilizes spill buckets (also called catchment basins) to recover drips or spills that may occur during delivery. The spill buckets should be large enough to contain the amount of fluid in the delivery hose.

Checklist

- ❐ 1. Are all delivery people aware of the type of overfill protection in use?
- ❐ 2. Do you keep fill ports locked, even when expecting delivery?
- ❐ 3. For delivery, do you unlock fill port and remain until delivery is complete?
- ❐ 4. Following delivery do you relock fill port and secure key?
- ❐ 5. Is the UST area secured to prevent access by unauthorized persons?
- ❐ 6. Do you regularly inspect the spill bucket to insure it is liquid-tight?
- ❐ 7. Do you make sure liquids do not accumulate in spill bucket?
- ❐ 8. Do you routinely remove dirt, rock, and other debris from spill bucket?
- ❐ 9. Do you do inspection and maintenance for cracks, holes, or other wear?
- ❐ 10. Do you keep an accurate inventory at all times?
- ❐ 11. Are overfill devices inspected regularly to ensure proper functioning?

Fail Safe Design

For many chemical storage containers fail-safe design is a crucial component of safety and security efforts. All system components are integrated to ensure that any single failure will cause the system to shut down safely.

Checklist

- ❐ 1. Can stored chemicals cause severe harm to humans or the environment?
- ❐ 2. Is this the best design for the chemical storage system being used?
- ❐ 3. Is the system regularly tested for reliability?
- ❐ 4. Is regular preventive maintenance performed?
- ❐ 5. Are operators all trained and tested on the use of the fail-safe system?
- ❐ 6. Do you have back up monitoring or surveillance?

Breakaway Couplings

Breakaway couplings prevent releases at separation points. Commonly installed in fuel dispensing systems, breakaway couplings prevent fuel spillage during drive away incidents. They may also reduce the likelihood of releases due to activity by vandals or criminals.

Checklist

- ❐ 1. Are couplings installed at all separation points?
- ❐ 2. Are couplings inspected regularly for wear or damage?
- ❐ 3. Are couplings replaced when needed?
- ❐ 4. Are couplings protected by other security methods?

Adequate Containment Systems

Secondary containment provides an additional layer of protection in case of spills, leaks, accidental or intentional releases. The containment materials should be as impervious as possible and compatible with the stored materials.

Secondary containment area is usually constructed to hold the entire contents of the largest tank or container within the containment area.

Checklist

- ❐ 1. Is the containment area constructed of impervious materials?
- ❐ 2. Is the containment material compatible with the product being stored?
- ❐ 3. Does the containment area have sufficient capacity to prevent overflow?
- ❐ 4. Is the containment area protected from rainfall and storm water flows?
- ❐ 5. Is the containment area inspected regularly for damage or wear?
- ❐ 6. Are the tanks or containers inspected regularly for damage or wear?
- ❐ 7. Are there back-up monitors, alarms or video surveillance?
- ❐ 8. Is there a written plan in case of containment failure?

Double-Walled Tanks

If properly maintained, double-walled tanks reduce the risk of leakage due to corrosion, wear, or physical damage.

Checklist

- ❐ 1. Are tank materials compatible with product stored?
- ❐ 2. Are automatic tank gauges installed to monitor tank contents?
- ❐ 3. Are interstitial fluid sensors installed to detect any leaks or seepage?
- ❐ 4. Do you manually check the interstitial space if there is no sensor?

Chemical Monitors

Continuous automated chemical monitoring is a very effective spill prevention tool. The monitors can indicate when less fuel is arriving than is being pumped. They can also be programmed to detect unauthorized releases or transfers and to notify appropriate personnel.

Checklist

- ❒ 1. Are monitors and valves programmed for automatic delivery shut down?
- ❒ 2. Do monitoring systems detect unauthorized releases or transfers?
- ❒ 3. Are notifications made automatically if the system detects a problem?
- ❒ 4. Are the monitors tested regularly for accuracy and operation?
- ❒ 5. Are the monitors checked regularly for failure or tampering?

Compressed and Liquefied Gases

Compressed gases pose a threat not only due to the contents, but also from the container itself.

Checklist

- ❐ 1. Are inside storage areas kept cool, dry, and well ventilated?
- ❐ 2. Do storage rooms have direct access to the outside?
- ❐ 3. Do storage rooms have a gas-tight barrier to prevent migration of gases?
- ❐ 4. Are storage areas secure from unauthorized personnel?
- ❐ 5. Are cylinders secured upright, bolted and double-chained?
- ❐ 6. Are valves kept closed with protective device in place?
- ❐ 7. Are oxygen cylinders stored at least 25 feet from incompatible materials? (flammable and combustible liquids or gases, oil and grease and LPG)
- ❐ 8. Are full and empty cylinders stored separately?
- ❐ 9. Does secure fencing enclose all outdoor storage areas?
- ❐ 10. Are all gates locked when area is unattended?
- ❐ 11. Are propane and other LPG tanks not in use stored outside?
- ❐ 12. Are gas pressure regulators used during delivery or system operation?
- ❐ 13. Are regulators appropriate for type and pressure of gas being used?

(Communications and Computers)

Multiple layers of security work very well when protecting communications and computer systems. Some layers will be to prevent unauthorized access at the location of the equipment. Other layers of protection will prevent unauthorized virtual access into all or parts of the systems.

Many times unauthorized access into communication and computer systems is committed by employees, ex-employees, friends or family of employees and contractors to the business. This group of people will usually have at least some limited access into the system and sometimes access to all parts of the system.

When physical access is authorized then theft of equipment becomes much easier than if the thief has to break in to steal. In person, while sitting at the computer is the easiest way to install software that can collect information for identity theft, intellectual property theft or surreptitious use of the system itself. The system should be arranged so a time/use audit, intrusion detection and/or intrusion prevention is available when authorized personnel are logged in.

Back up for communications and computer systems includes the operations location, the equipment, the data generated or used by the equipment and/or the power source used by the equipment. A spare building with unused auxiliary equipment is probably not an alternative for the average small business. There may be another business that could accommodate your operation if you needed to relocate in an emergency. You may be able to operate from home, a community Library, a Community College or a company like FedEx Kinko's. This can work if you have access to current backed-up data.

Depending on the type of business, with current software, current company data, a wireless enabled laptop computer and a cell phone, operations could continue from free WiFi locations or many businesses like Starbucks or a McDonald's where they also provide access to wireless Internet connections for a fee.

You may have or need to have alternative sources of power including diesel-powered generators or a battery system, both of which come in many sizes. This may be power for your entire operation, just the essentials such as communications and computers or just enough to back-up current information and shut down the system without damage.

Checklist

- ❒ 1. Can you identify multiple layers of security?
- ❒ 2. Do you have certified IT Security people on staff or contract?
- ❒ 3. Does your company have an access control system in place?
- ❒ 4. Do you have additional physical barriers like locked doors?
- ❒ 5. Do you have physical intrusion detection for equipment?
- ❒ 6. Do you have a system for password generation and control?
- ❒ 7. Do you have firewalls, intrusion detection and prevention?
- ❒ 8. Are your security systems and procedures tested regularly?
- ❒ 9. Do you have appropriate back-up power supplies?
- ❒ 10. Is back-up power tested regularly?
- ❒ 11. Do you have off-site operations alternatives available?
- ❒ 12. Do you have critical data backed up off-site consistently?
- ❒ 13. Do you have a back-up communications plan?
- ❒ 14. Do you have back-up communications equipment available?
- ❒ 15. Do you test your emergency communications plan?

(Personnel – Employees And Contractors)

Aggressive Background Checks

Certain occupations, such as security-sensitive positions or working with children, require background checks. For other positions, employers are often hesitant to conduct background checks. However, by checking backgrounds of potential employees, you may avoid many pitfalls.

Studies have shown that 80% of network security breaches occur from the inside, 18% of job applicants lie about criminal records, 29% lie about their education, 25% misrepresent their employment history, and 23% have used other names for fraudulent purposes.

Businesses frequently contact former employers as part of the hiring process. However, due to the fear of lawsuits, many companies have a policy limiting information on former employees to dates of employment. Therefore, conducting at least a minimal background check may be necessary to protect your business and other employees. Some commonly conducted checks include credit (to identify applicants whose financial situation might motivate them to steal from the company), education and licenses (to verify qualifications), and criminal record (to protect employees and customers and to avoid negligent hiring lawsuits).

Checklist

- ❒ 1. Do you use extensive background and reference checks?
    - Social Security records
    - State driving records
    - Credit reports
    - Past employment history
    - Formal education
    - Occupational and professional licenses
    - Criminal records
    - Military records
    - Allowed to work status in the United States
    - Character references
- ❒ 2. Do you use a release form authorizing checks of sources and records?
- ❒ 3. Are checks conducted internally or by an independent agency?
- ❒ 4. Do company background checks comply with state and federal laws?

Drug Screening

Drug-Free America Foundation, Inc. estimates substance abuse cost business owners an estimated $100 billion annually in absenteeism and tardiness, accidents, and insurance costs. Drug screening will help avoid employing people with substance-abuse problems. It may assist your company with identifying current employees with substance abuse problems.

A study conducted by the Substance Abuse and Mental Health Services Administration (SAMHSA) in 2002 found that 74.6% of illicit drug users were employed either part-time or full-time. It has also been shown that most of those people are employed by small businesses. This is largely due to a lack of drug testing and drug-free workplace (DFWP) policies and programs.

Pre-employment drug testing will substantially reduce the number of applicants who use drugs. More reductions can be gained through random testing of employees. If employees don't know when they will be tested its much harder for the employee to "cheat". Many companies also use post-accident and "for cause" testing, particularly if there are substantial safety or security risks.

Drug screening must be applied equitably among all employees and management. An Employee Assistance Program if offered should be available to all employees equally. Your company policy should clearly state the consequences of violating the DFWP policy. Violations should be dealt with according to the policy.

Checklist

- ❒ 1. Do your applicants take a pre or post employment drug test?
- ❒ 2. Do you have an ongoing program to test employees for drug use?
- ❒ 3. In the event of an accident, do you test all employees involved?
- ❒ 4. Do you test employees based on behavior or performance indications?
- ❒ 5. Do you offer an Employee Assistance Program (EAP) to employees?
- ❒ 6. Does your policy allow for treatment and successful rehabilitation?
- ❒ 7. Are positive test results verified before taking any action?

Pre or Post Hire Physicals

Many companies have found that medical exams can reduce injuries and illnesses resulting in lower workers' compensation costs. Physical exams and hearing tests can be used to establish a baseline and limit future liability. They may also serve to identify conditions which may affect an employee's health, ability to work, or need for reasonable accommodation.

When dealing with job applicants, employers should be aware that the Americans with Disabilities Act (ADA) prohibits asking disability-related questions or requiring medical exams until after the applicant has been given a conditional job offer. Employers can require applicants to perform actual or simulated job tasks to demonstrate ability to do the job. Applicants with disabilities may not be excluded if they can perform the essential functions with reasonable accommodation.

Checklist

- ❒ 1. Do your employment applications and interviews comply with ADA?
- ❒ 2. Do job simulations determine ability to perform essential functions?
- ❒ 3. Do post-hire physicals identify risks and avoid future illness/injury?
- ❒ 4. If an applicant is rejected because of a disability, can you demonstrate the rejection is "job related and consistent with business necessity"?
- ❒ 5. If a disabled applicant is rejected for safety reasons, can you show that the risk could not be reduced to acceptable levels through reasonable accommodation?
- ❒ 6. Are all new employees in the same job category required to take the same medical exams?
- ❒ 7. Is all medical information kept confidential?

Termination for False Information

Some companies have a policy of termination if they determine an employee has given false information on an employment application or other document. This is based on the premise that the false information is indicative of a character trait, and the employee may be dishonest in other areas as well. This policy provides grounds for termination if a company suspects an employee of dishonesty or unethical behavior on the job, but has no proof. However, it removes flexibility in dealing with a good employee who poses no risk to the company and may be difficult to replace.

Checklist

- ❒ 1. Is your company's policy, automatic termination for false information?

- ❒ 2. Does your company attempt to verify all information on applications prior to making a job offer?

Chapter 3

Policies and Procedures

Posted Security Plan

Every business, regardless of size, should have a written security plan for dealing with potential emergency situations. Emergencies may arise due to natural or man-made disasters, and your plan should address both. This book concentrates on the vandal/terrorist caused disasters; however, much of the information will be applicable to other disaster types as well.

You should begin by identifying potential hazards and vulnerabilities associated with your business. (See Chapter 4, Site Specific Security Factors.) Then identify internal and external resources available to prevent or respond to potential threats. Once the plan has been written, provide employees with copies of the plan, and train them on procedures and any specific responsibilities. Periodically evaluate the plan and revise as needed. Post support documents (emergency call lists, resources lists, maps) throughout the facility for quick access.

Following is an outline based on the *Emergency Management Guide for Business and Industry*, developed by the Federal Emergency Management Agency (FEMA). Note that the Guide consists of recommendations, not regulations. The complete guidance document can be located on the Internet at the following address: http://www.fema.gov/pdf/library/bizindst.pdf

Security Plan Outline

- Executive Summary

- ❒ Purpose of the plan
- ❒ Facility's emergency management policy
- ❒ Authorities and responsibilities of key personnel
- ❒ Types of emergencies that could occur
- ❒ Where response operations will be managed

- Emergency Management Elements

- ❒ Direction and control
- ❒ Communications
- ❒ Life safety
- ❒ Property protection
- ❒ Community outreach
- ❒ Recovery and restoration
- ❒ Administration and logistics

- Emergency Response Procedures (in the form of checklists)

- ❒ Assessing the situation
- ❒ Protecting employees, customers, visitors, equipment, vital records and other assets; may include:
  - Procedures for reporting emergencies.
  - Warning employees and customers
  - Communicating with personnel and community responders
  - Emergency escape procedures and routes
  - Procedures for employees who perform or shut down critical operations before an evacuation
  - Procedures to account for all employees, visitors, and contractors after an evacuation is completed
  - Rescue and medical duties for assigned employees
  - Managing response activities
  - Activating and operating an emergency operations center
  - Fighting fires
  - Names of persons or departments to be contacted for information regarding the plan.

- Restoring operations and other actions for getting the business back up and running
- Support Documents

- ❒ Emergency call lists (24-hour phone numbers)
- ❒ Outside resource lists (private companies and government agencies who could assist in emergency situations)
- ❒ Building and site maps which include:
  - Utility shutoffs
  - Water hydrants
  - Water main valves
  - Water lines
  - Gas main valves
  - Gas lines Electrical Cutoffs
  - Electrical Substations
  - Storm drains
  - Sewer lines
  - Location of each building
  - Floor plans
  - Alarm and enunciators
  - Fire extinguishers
  - Fire suppression systems
  - Exits
  - Stairways
  - Designated escape routes
  - Restricted areas
  - Hazardous materials
  - High-value items

Incident Reporting System

Your facility should have a written plan for reporting security-related incidents, including crime, medical emergency, threats, fire, weather-related events, and chemical/biological hazards. The plan should detail how reported incidents are handled and how information is communicated to employees and visitors. Employees should be provided with copies of the plan and trained on the procedures.

Checklist

- ❐ 1. Do you have a written plan for reporting security-related incidents?
- ❐ 2. Do employees have access to the plan, and training in the procedures?
- ❐ 3. Does your facility have 24 hour on-site security personnel?
- ❐ 4. Does your plan include incidents that occur outside of normal working hours?
- ❐ 5. Does your plan include local police, fire departments, or other resources?
- ❐ 6. Do you have a public address system or other means for notifying building occupants of emergency situations and necessary actions?
- ❐ 7. Does the plan include accommodations for notifying and assisting disabled individuals?
- ❐ 8. Are reported incidents and outcomes documented?
- ❐ 9. Is there a system for analyzing incident reports to identify trends and possible corrective actions?

EPA Risk Management Plan (RMP)

Section 112(r) of the Clean Air Act (CAA) requires facilities with more than a threshold quantity of a listed extremely hazardous substance to submit a risk management plan (RMP) to the EPA, electronically or on paper. RMPs must be resubmitted every five years or if certain changes happen, whichever comes first.

Regulations and guidance documents are located on the EPA website, http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/RMPS.htm?OpenDocument Specific guidance on the RMP is located at http://yosemite.epa.gov/oswer/ceppoweb.nsf/vwResourcesByFilename/Chap-09-final.pdf/$File/Chap-09-final.pdf

RMP Outline

Any facility with one or more covered processes must include in its RMP:

- Executive summary (§ 68.155)
- Registration for the facility (§ 68.160)
- Certification statement (§ 68.185)
- Worst-case scenario analysis for each Program 1 process; at least one worst-case scenario analysis to cover all Program 2 and 3 processes involving regulated toxic substances; at least one worst-case scenario analysis to cover all Program 2 and 3 processes involving regulated flammables (§ 68.165(a))
- Five-year accident history for each process (§ 68.168)
- Information concerning emergency response at the facility (§ 68.180)

Any facility with at least one covered process in Program 2 or 3 must include:

- At least one alternative release scenario analysis for each regulated toxic substance in Program 2 or 3 processes and at least one alternative release scenario analysis to cover all regulated flammables in Program 2 or 3 processes (§ 68.165(b))
- Summary of the prevention program for each Program 2 process (§ 68.170)
- Summary of the prevention program for each Program 3 process (§ 68.175)

A definition of program levels and flow chart for determining the program level of individual processes can be found in Chapter 2 of the EPA guidance document: http://yosemite.epa.gov/oswer/ceppoweb.nsf/vwResourcesByFilename/Chap-02-final.pdf/$File/Chap-02-final.pdf

OSHA General Duty Clause

Section 5(a)(1) of the Occupational Safety and Health (OSH) Act requires employers to provide a safe and healthful workplace "free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees". This section, also known as the "General Duty Clause", requires employers to address workplace hazards even if there are no regulations specifically pertaining to those hazards. The Act was originally passed to address traditional occupational hazards related to machinery, exposure to disease, and other working conditions. However, as terrorism is now a "recognized hazard" in this country, employers may be held responsible for taking action to protect workers from injury due to terrorist attacks. The level of preventive action necessary will depend upon factors such as the specific nature and location of the business.

Checklist

- ❒ 1. Is employee safety a priority at your facility?
- ❒ 2. Do you employ a safety manager?
- ❒ 3. Does the Safety Manger have potential conflicts, like production goals?
- ❒ 4. Do you provide safety training to employees on a regular basis?
- ❒ 5. Does your company know and comply with current safety regulations?
- ❒ 6. Is your company proactive with policies to prevent injuries?
- ❒ 7. Does your company routinely perform job safety analyses?
- ❒ 8. How do existing security measures protect employee safety?
- ❒ 9. What additional measures could be taken to increase employee safety?

Labor Relations

Labor relations can directly impact the security of your company and its workforce. Strikes and shutouts can result when issues are not resolved in a reasonable manner. Labor relations are important in non-union workplaces too.

Disgruntled employees and contractors have committed actions including workplace violence, violation of trade secrets, theft, and vandalism. These actions can do serious damage to a company. More common is the spreading of negative information about the company. Internet "employer bashing" can have severe effects on a company's finances and reputation. There are Websites and message boards only providing insiders' views, where employees anonymously post opinions or experiences regarding specific companies. These comments, which tend to be negative, are accessible to anyone.

Some employers now monitor their employees' Internet and email usage, which is currently a very controversial issue. Monitoring proponents claim that it increases productivity and protects them from viruses, harassment lawsuits, and leaks of confidential information to competitors. Opponents claim it violates workers' right to privacy, increases company liability, and constitutes inefficient use of HR and IT personnel. Employees should be provided with written guidelines or policies regarding Internet and email usage.

Checklist

- ❒ 1. Do your employment policies and practices prohibit discrimination?
- ❒ 2. Do your policies and procedures prevent and stop sexual harassment?
- ❒ 3. Does your company have a written policy for employee grievances?
- ❒ 4. Are policies enforced equitably among all employees?
- ❒ 5. Do employees sign agreements to not disclose confidential information?
- ❒ 6. Does management keep open lines of communication with employees?
- ❒ 7. Does your company monitor employees' Internet and email usage?
- ❒ 8. Does your company have a written computer use policy?
- ❒ 9. Do you monitor your company's Internet image?
- ❒ 10. Do employees counter negative information if inaccurate or unjustified?

Workplace Violence

The OSHA definition of Workplace violence is “any physical assault, threatening behavior, or verbal abuse occurring in the workplace”. Perpetrators may be strangers, co-workers, customers or personal relations. OSHA statistics show workplace violence as the “third-leading cause of fatal occupational injury in the United States”. The Bureau of Labor Statistics reports that, of a total of 8,786 fatal work injuries in 2001, 639 were homicides.

Certain industries or working conditions are more prone to workplace violence incidents. The Centers for Disease Control (CDC) identified the following factors as indicating a higher than average risk of workplace violence:

- Contact with the public
- Exchange of money
- Delivery of passengers, goods, or services
- Having a mobile workplace such as a taxicab or police cruiser
- Unstable or volatile co-workers in health care, social service, or criminal justice settings
- Working alone or in small numbers
- Working late at night or during early morning hours
- Working in high-crime areas
- Guarding valuable property or possessions
- Working in community-based settings

OSHA recommends conducting an in-depth review of your workplace to identify conditions that may lead to workplace violence, then putting together a program to prevent and deal with violence. A sample plan, written by the Long Island Coalition for Workplace Violence Awareness and Prevention (LICWVAP), is posted on the OSHA website:

http://www.osha.gov/workplace_violence/wrkplaceViolence.PartIII.html

Workplace Violence: Issues in Response, a guide produced by the FBI's National Center for the Analysis of Violence Crime (NCAVC) is available online at

http://www.fbi.gov/publications/violence.pdf.

This document lists the following components of a workplace violence prevention program:

- A statement of the employer's no threats and violence policy and complementary policies such as those regulating harassment and drug and alcohol use.
- A physical security survey and assessment of premises.
- Procedures for addressing threats and threatening behavior.
- Designation and training of an incident response team.
- Access to outside resources, such as threat assessment professionals.
- Training of different management and employee groups.
- Crisis response measures.
- Consistent enforcement of behavioral standards, including effective disciplinary procedures.

Checklist

❒ 1. Are your company managers and top executives committed to preventing workplace violence and doing away with conditions that may be conducive to violent interactions?

❒ 2. Are you willing/able to change conditions in the workplace culture that increase the risk of violence? (e.g. tolerance of bullying or intimidation, high stress levels, poor communication, inconsistent enforcement of company policies, etc.)

❒ 3. Do you conduct pre-employment screenings to identify risk factors such as substance abuse, previous conflicts with coworkers, and criminal convictions?

- ❒ 4. Do you look for signs of problem behavior in current and potential employees using what the FBI document lists as “red flags”:
  - Increasing belligerence
  - Ominous, specific threats
  - Hypersensitivity to criticism
  - Recent acquisition/fascination with weapons
  - Apparent obsession with a supervisor or coworker or employee grievance
  - Preoccupation with violent themes
  - Interest in recently publicized violent events
  - Outbursts of anger
  - Extreme disorganization
  - Noticeable changes in behavior
  - Homicidal/suicidal comments or threats

- ❒ 5. Do you try to eliminate or minimize stressful working conditions?
  - Understaffing
  - Poorly defined tasks and responsibilities
  - Downsizing/reorganization
  - Poor labor relations
  - Poor management styles
  - Inadequate security
  - Lack of employee counseling
  - High injury rates or frequent employee grievances

- ❒ 6. Do you periodically survey employees regarding security concerns?

- ❒ 7. Have you identified and evaluated changes in the building layout that can increase visibility, control access, or provide escape routes for employees?

- ❒ 8. Do you have a policy for assessing and addressing threats and threatening behavior?

- ❒ 9. Do you have legal and law enforcement resources available for difficult situations?

- ❒ 10. Do you provide training to employees in the following areas?

  - Workplace violence prevention policy
  - Incident reporting system
  - Recognizing risk factors and warning signs
  - Responses to diffuse threats and threatening behavior
  - Cultural diversity
  - Location and operation of alarms and other safety devices
  - Personal safety

Substance Abuse

Studies of substance abuse in the workplace have consistently documented that substance-abusing employees take more sick days, have lower productivity, have more accidents, and file more workers' compensation claims, than non-using employees. The Drug Free America Foundation (DFAF) estimates that substance abuse by employees costs American businesses $100 billion per year in the form of higher absenteeism, tardiness, accidents, and insurance costs.

According to the 2002 National Survey on Drug Use and Health (NSDUH), conducted by the Substance Abuse and Mental Health Services Administration (SAMHSA), 74.6% of illicit drug users age 18 or over were employed either full or part-time. The survey indicated that 80% of adult binge drinkers were employed, and 79% of adult heavy drinkers were employed.

Employers can greatly reduce the personnel-related risks to their businesses by implementing Drug-Free Workplace Programs (DFWP). At a minimum, a DFWP should consist of a Drug-Free Workplace Policy. Additional recommended components include:

- Supervisor training
- Employee education
- Employee assistance
- Drug testing

Small business owners should be aware that they employ a disproportionately high number of substance abusers because small businesses typically do not have programs in place to identify and deal with substance abuse in employees and applicants.

The Department of Labor website has an interactive tool to help businesses develop a DFWP. (See http://www.dol.gov/elaws/asp/drugfree/drugs/screen2.asp.) This tool helps employers to evaluate and formulate each of the five components of a DFWP.

Checklist

- ❒ 1. Does your company have a drug-free workplace policy?
- ❒ 2. Does the policy prohibit use of alcohol and drugs in the workplace?
- ❒ 3. Does the policy encourage employees to seek help with alcohol and drug problems?
- ❒ 4. Has the policy been communicated and explained to all employees?
- ❒ 5. Are alleged violations investigated and employees allowed to respond?
- ❒ 6. Does the policy conform to union contracts and federal and state laws?
- ❒ 7. Does the policy include measures to ensure confidentiality?
- ❒ 8. Is the policy enforced equitably for all employees?
- ❒ 9. Do you conduct drug testing? Are positive tests verified?
- ❒ 10. Does the policy specify when drug tests will be conducted?
- ❒ 11. What are the consequences of a positive test?
    - Referred to counseling/treatment
    - Suspension or other disciplinary action
    - Reassignment to other duties
    - Immediate termination
    - Retesting following completion of treatment
    - Termination following second positive test
- ❒ 12. Do company benefits include an employee assistance plan (EAP)?
- ❒ 13. Are all supervisors fully trained in use of the drug-free policy?
    - Supervisors' responsibilities in implementing the policy
    - Recognizing signs of possible substance abuse
    - Dealing with employees who may have substance abuse problems.

Monitored or Limited Inventory

Maintaining limited inventories can reduce the risk of vandalism, robberies, or break-ins. Depending on the material being stored, this may reduce the risk of damage due to accidents or weather events. Regardless of the amount of inventory maintained, businesses should keep adequate records to detect shrinkage or unexplained variances. A wide variety of inventory software is currently available and applicable to most industries. Some companies prefer to maintain manual inventory logs.

Manufacturers storing or using hazardous or security-sensitive chemicals can reduce their risks by utilizing a form of just-in-time acquisition. Chemical management services (CMS), also known as total chemical management (TCM), allows businesses to shift the risks and liability associated with chemical storage to their suppliers. Due to their higher volumes, suppliers should already have safeguards in place to protect against criminal activity, accidents, and natural disasters. Deliveries are timed so that the chemicals arrive just prior to when the customer needs them. This system is particularly beneficial when dealing with shock sensitive chemicals, or chemicals that may become shock sensitive when stored improperly or for a prolonged period of time.

Additional benefits of CMS include reduced recordkeeping and reporting, less space required for storage, lower disposal costs, and lower insurance costs.

Checklist

- ❒ 1. Do you have a system in place to accurately track inventories?
- ❒ 2. Do you use hazardous chemicals attractive to thieves or drug dealers?
- ❒ 3. Have you discussed just-in-time delivery options with your suppliers?
- ❒ 4. Can you calculate needs accurately and implement a CMS program?

Data Back-up

One necessity to protect your business against hard drive crashes, viruses, worms, and human error is to back up your data daily or as needed.

Once a week or more often if needed, backup copies should be stored off-site to ensure access to a recent copy of files in case of a disaster. You may want to electronically transfer data to a third party.

Checklist

- ❒ 1. Have you determined how frequently you need to back up your data?
- ❒ 2. Have you determined what media you will use for backup?
  - Floppy disk or Zip drive
  - CD or DVD
  - Alternate hard drive
  - Tape drive
  - Flash disk
  - Colocation service provider
  - Internet backup
- ❒ 3. What type of backups are conducted, and how often?
  - Full backup – all files on the system
  - Differential backup – files changed since last full backup
  - Modified backup – files changed since last full or differential backup
- ❒ 4. Are you conducting backups daily or as needed?
- ❒ 5. Do backups run automatically or are they conducted manually?
- ❒ 6. Are copies stored off-site weekly or as needed?
- ❒ 7. Are backups tested regularly to ensure correct data is available?
- ❒ 8. Do you review backup log files for indications of problems with backup?

Contingency Plan

All businesses should have a contingency plan that specifies how to prepare for, respond to, and recover from business interruptions. Interruptions may come in the form of natural disasters, chemical or biological exposure, mechanical or technological failure, human error, terrorist activities, or a combination of various factors. Therefore, contingency planning should take an “all hazards” approach.

The first step in developing a contingency plan is to assess the risks faced by the business. It is not necessary to try to identify every potential event that could cause a business interruption. You will notice that completely different events often have very similar effects on your business.

Identifying these effects will form the basis for conducting a Business Impact Analysis (BIA), the second step in the planning process. You will need to determine what are your business’ most critical products, services and processes. The BIA consists of identifying and assessing the severity of potential losses (financial and otherwise). Impacts affecting critical products, services and processes should receive the highest priority. Some critical impacts may be external to the business. What would be the effect if critical services are provided to a local customer base and the customer base is relocated?

Once you have analyzed these potential impacts, you can begin the task of deciding how you will prepare for and respond to these events. This step will also include planning for resuming operations and recovering from the interruption. It is likely that following a serious business interruption event that just doing what you did before will not work. The external changes will probably require internal changes as well.

Finally, the plan should be practiced through periodic drills or training exercises. The plan should be evaluated and revised as needed on an ongoing basis.

Checklist

- ❒ 1. Using an “all hazards” approach, have you identified and analyzed threats and vulnerabilities that could lead to a business interruption?
- ❒ 2. Have you identified critical products, services and processes for your business?
- ❒ 3. Do you have a business impact analysis (BIA) that identifies and ranks business impacts?
- ❒ 4. Does your plan include preventing the likelihood of interruptions, and minimize damage?
- ❒ 5. Do you have emergency generators or other alternate power sources?
- ❒ 6. Do you have arrangements for an alternate work site to continue operation if facility is inoperable or inaccessible?
- ❒ 7. Do you have arrangements to obtain needed equipment on short notice?
- ❒ 8. Do you have arrangements to contract operations on a temporary basis?
- ❒ 9. Are critical documents and data stored off-site, secured and accessible?
- ❒ 10. Is a critical back up communications system in place?
- ❒ 11. Are employees, customers, and suppliers trained on back up?
- ❒ 12. Do you keep and store off-site a complete inventory for insurance?
- ❒ 13. Does your plan document damage, protect undamaged property, and reclaim salvageable property?
- ❒ 14. Do you have a public relations plan for communicating with the media?

Responding Agencies

Companies should familiarize themselves with community emergency response organizations and involve them in planning for emergencies. Businesses that use, store, or produce specified quantities of hazardous substances are required to report to state and local regulatory and emergency response organizations. However, it is in the best interest of most businesses' to ensure local emergency response organizations are informed about any potential hazards associated with their business.

Depending on your facility size, location, and nature of business, you may need to include community emergency response organizations in planning, training and drills. A key organization when planning for chemical-related contingencies is the Local Emergency Planning Committee (LEPC). This committee consists of representatives of the following groups and organizations:

- **Elected and local officials;**
- **Law enforcement;**
- **Civil defense;**
- **Firefighting;**
- **First aid;**
- **Health;**
- **Local environmental and transportation agencies;**
- **Hospitals;**
- **Broadcast and print media;**
- **Community groups; and**
- **Representatives of facilities subject to the emergency planning and community right-to-know requirements.**

Checklist

- ❒ 1. Have you identified community emergency response organizations?
- ❒ 2. Have you communicated the amounts and locations of any hazardous substances used or stored (even temporarily) at your facility?
- ❒ 3. Have you provided responding agencies with maps of your facility, showing utility lines and locations of any hazardous materials?
- ❒ 4. Have you involved emergency response organizations in contingency planning and training for your facility?
- ❒ 5. Do you conduct periodic drills to test your plan and to ensure employees are familiar with procedures?
- ❒ 6. Do you test the plan in segments to ensure nothing is overlooked?
- ❒ 7. Have you requested responding agency participation in drills?

Preventive Maintenance

Having a well-maintained facility and equipment is critical to your business' security. The effectiveness of any security measure is compromised if not properly maintained. Additionally, improperly maintained equipment can become a security hazard.

Checklist

- ❒ 1. Have you developed a maintenance schedule for each piece of equipment, based on manufacturer's recommendations?

- ❒ 2. Do you prohibit repairs or making modifications to any equipment unless authorized by the manufacturer to do so?

- ❒ 3. Do you regularly inspect the entire facility and all equipment for signs of wear or damage which could compromise safety, integrity or security?

- ❒ 4. Do you have equipment inspection checklists that must be completed before each use or shift?

Cleaning Staff or Contractor

Janitorial services are often provided by outside contractors. In many office buildings or other leased facilities, cleaning services are contracted by the building management with no input from individual companies. Whether your company utilizes employees or contractors, janitorial service can be a security risk due to the level of access and work that is typically done after business hours. The lack of supervision and high turnover rate can result in intentional or accidental breaches of security.

Checklist

- ❒ 1. Do you require the contractor to be bonded and to conduct background and criminal checks on their employees?

- ❒ 2. Do you require the contractor to provide a current employee list before each shift and have each employee sign in?

- ❒ 2. Do you conduct thorough background and criminal checks on employees?

- ❒ 3. Do you check all references of cleaning contractors or employees?

- ❒ 4. Do you require cleaning staff to leave outside doors and unattended offices locked at all times?

- ❒ 5. Do you provide cleaning staff with after-hours contact numbers, and require they report any unusual or suspicious activity?

- ❒ 6. Do you provide ongoing training on upholding security standards?

- ❒ 7. Do you regularly monitor janitorial staff to ensure they are following procedures?

Chapter 4

SITE SPECIFIC SECURITY FACTORS

Image Portrayed by Company

Terrorists or criminals motivated by ideology often use a high profile public image to select their targets. In addition to the tremendous loss of life and damage to property, the 2001 attacks on the World Trade Center and the Pentagon were attacks on the U.S. economy and military. An attack on the White House, which was reported to be the mission of the third hijacked airplane, would signify an attack on the President and the government in general.

Signs, marketing efforts, or recent publicity, either positive or negative, may depict the public image of your business. The name of your company, the products and services you provide are factors that can affect your business' image and security.

Include public image of your company or industry in your vulnerability assessment. Use the analysis from that to determine the need to lower your company's profile in the community.

Checklist

- ❒ 1. Is your company (or industry) controversial in any way?
- ❒ 2. Is there recent publicity on your company, competitors or the industry?
- ❒ 3. Could prominent signage increase security risks for your company?
- ❒ 4. Do subsidiaries use the parent company name on their signage?
- ❒ 5. Are any of your products or services considered harmful or immoral?
- ❒ 6. Is your company name or logo depicted as bad by any groups or persons?

Significant Location or Surrounding Area

Densely populated areas, nearby government facility or building, historic landmarks, military installations, birth control clinics, hospitals, police stations, energy company headquarters and energy producing facilities are all part of a list usually considered to be a high security risk.

If one of those facilities has their security compromised then nearby facilities may be damaged to an equal or greater extent than a targeted facility. Your vulnerability assessment should consider risk due to surrounding land use and should be considered when deciding where to locate a new business.

Checklist

- ❒ 1. Are you located in or near a major city or metropolitan area?
- ❒ 2. Are there federal, state, or local government facilities in the vicinity?
- ❒ 3. Are there military installations or large defense contractors nearby?
- ❒ 4. Are you near a police or medical facility?
- ❒ 5. Are there any historic sites or monuments close to your business?

Political in Nature

Does your company offer products or services that are opposed by political, social, or religiously motivated individuals or groups? Many people are willing to use violence or threats of violence as a means to their end objective. This situation will be countered by an assessment of the risk and the plan to put appropriate layers of protection in place.

Companies involved in international trade may also be targeted for political or social reasons. It is possible to face the same types of risk if your business is perceived to promote a political, social, or religious agenda. The same analysis should be done and the necessary precautions should be implemented.

Checklist

- ❐ 1. Is your business related to any volatile or divisive issues?
- ❐ 2. Do your products or services support (or appear to support) one side of a controversial social issue?
- ❐ 3. Have the owners or managers of your company taken a public stance on a controversial issue?
- ❐ 4. Does your company contribute to political, social, or religious organizations?
- ❐ 5. Has your company stopped donating to an organization because of political, social, or religious controversy?
- ❐ 6. Does your company import products that compete with American goods?
- ❐ 7. Does your company conduct business with a foreign country that is perceived as violating human rights?
- ❐ 8. Does your company or industry currently do off-shoring of jobs?
- ❐ 9. Has your company recently had lay-offs?

Chemicals or Equipment

The presence of hazardous or potentially hazardous chemicals or heavy equipment can make your facility attractive to vandals or terrorists. Criminals may use the equipment to create an explosion or chemical release at your facility. Or they may steal the chemicals for use elsewhere. Terrorists and other criminals are often able to create bombs and drugs from common household materials.

Retailers should be aware of equipment and components frequently found in methamphetamine labs:

- Pool acid/ Muratic acid
- Lye
- Acetone
- Brake Fluid
- Brake Cleaner
- Iodine Crystals
- Lithium Metal / Lithium Batteries
- Lighter Fluid
- Drain Cleaners (Drano or Liquid Fire)
- Cold Medicine Containing Pseudoephedrine or Ephedrine
- Ethyl Ether (Starting Fluid)
- Anhydrous Ammonia (stored in propane tanks or coolers)
- Sodium Metal
- Red Phosphorus
- Ephedrine
- Laboratory Glassware
- Coffee Filters

Manufacturers and distributors should be aware that they are required to abide by provisions regulating the following chemicals:

- Acetic Anhydride (CAS NO. 108-24-7)
- Benzaldehyde (CAS NO. 100-52-7)
- Benzyl Chloride (CAS NO. 100-44-7)
- Benzyl Cyanide (CAS NO. 140-29-4)
- Diethylamine and its salts (CAS NO. 109-89-7)
- Ephedrine, its salts, optical isomers and salts of optical isomers (CAS NO. 299-42-3)
- Hydriodic Acid (CAS NO. 10034-85-2)
- Iodine (CAS NO. 7553-56-2)
- Lithium (CAS NO. 7439-93-2)
- Methylamine and its salts (CAS NO. 74-89-5)
- Nitroethane (CAS NO. 79-24-3)
- Chloroephedrine, its salts, optical isomers and salts of optical isomers (CAS NO. 30572-91-9)
- Phenylacetic Acid, its esters and salts (CAS NO. 103-82-2)
- Phenylpropanolamine, its salts, optical isomers and salts of optical isomers (CAS NO. 14838-15-4)
- Piperidine and its Salts (CAS NO. 110-89-4)
- Pseudoephedrine, its salts, optical isomers and salts of optical isomers (CAS NO. 90-82-4)
- Red Phosphorous (CAS NO. 7723-14-0)
- Sodium (CAS NO. 7440-23-5)
- Thionylchloride (CAS NO. 7719-09-7)

Checklist

- ❒ 1. Are safeguards in place to secure chemicals and equipment? (See Chapter 2.)

- ❒ 2. Are you familiar with, and compliant with, the Comprehensive Methamphetamine Control Act of 1996 (MCA) and the Methamphetamine Anti-Proliferation Act of 2000?

- ❒ 3. Do you limit sale quantities of common methamphetamine components (applies particularly to pharmacies, grocery stores, discount stores, convenience stores, and agricultural cooperatives)?

- ❒ 4. Do you report “suspicious orders” of listed chemicals?

- ❒ 5. Do you watch for suspicious activity around anhydrous ammonia tanks?

Location, Age, and Type of Building

Your security needs will depend to some extent on building specifics. Older buildings may require some renovations before installing some of the newer, automated security systems. Proper maintenance is essential, regardless of the age of your building. A building that appears neglected is more likely to be targeted. It is also important to remove any results of vandalism as soon as possible by painting over graffiti and replacing damaged signs or equipment.

Checklist

- ❐ 1. Have you verified building blueprints and drawings for accuracy?
- ❐ 2. Do you maintain and test security measures on a regular basis?
- ❐ 3. Do you require employees and contractors to always use existing security devices? (locking doors and windows, setting alarms, etc.)
- ❐ 4. Are HVAC systems installed correctly and have correct type filters?
- ❐ 5. Have you installed low-leakage fast-acting outdoor air dampers?
- ❐ 6. Have you provided ground-level air intakes with security protection?
- ❐ 7. Have you made any changes, adjustments or modifications that may have adverse effects on building operation or employee health and safety?
  - Sealing outdoor air intakes
  - Unauthorized modifications to HAVC system
  - Altering fire protection systems or escape routes
  - Using high-efficiency filters not compatible with existing HVAC system.
- ❐ 8. Do you have secure access to HVAC and other building system controls?
- ❐ 9. Do you restrict access to critical building information?

Hours of Operation

Businesses that are open late at night and early morning have an increased risk of robbery and workplace violence. This risk increases if employees work alone, in small groups or in high crime areas. Following are some options recommended by OSHA to protect late night/early morning workers.

Checklist

- ❒ 1. Have you improved visibility with adequate lighting, installed mirrors and keep signs and shelves low in windows?
- ❒ 2. Do you use drop safes and signs that indicate little cash is kept on-hand?
- ❒ 3. Does the businesss have video surveillance ?
- ❒ 4. Do you provide silent and personal alarms?
- ❒ 5. Do you provide emergency communications, training and education?
- ❒ 6. Do you restrict customer access by reducing store hours and closing portions of a store?
- ❒ 7. Do you have security procedures for remote or isolated spots such as garbage areas and outdoor freezers?
- ❒ 8. Are all doors not in use kept locked?
- ❒ 9. Do you increase staffing during high-risk periods?
- ❒ 10. Have you installed bullet-resistant enclosures?

Organize A Neighborhood Business Watch

A business watch operates much the same as a neighborhood crime watch. Rather than focusing strictly on their own property, business owners and employees look out for each other as well. By becoming familiar with neighboring businesses and their routines, people are better able to recognize suspicious activity. A business watch can be a major factor in deterring or solving crimes and consequently helping workers and customers to feel more secure.

Checklist

- ❐ 1. Do you know neighboring businesses' hours of operation?
- ❐ 2. Are your employees alert and always report suspicious behavior?
- ❐ 3. Have you developed a phone tree to transmit important information among the group easily and efficiently?
- ❐ 4. Have you included local law enforcement for assistance with security surveys, advice on lighting, alarms, locks, and other security measures?
- ❐ 5. Have you marked all equipment with your tax ID or other identification number using a system that prevents removal of the number?
- ❐ 6. Do you publicize the business watch to criminals by posting signs in conspicuous locations throughout the watch area?
- ❐ 7. Do you work with community partners such as chambers of commerce, industry or business associations and service clubs?