Business Crime Prevention Handbook

Tools & techniques to keep your business property crime free

Snohomish County Sheriff’s Office | Crime Prevention Unit
425-388-7375 | crimeprevention@snoco.org | http://sheriff.snoco.org
# Table of Contents

Introduction to Business Crime Prevention .................................................. 3
Burglary ........................................................................................................... 5
Check Fraud/Counterfeit Money ................................................................. 6
Crime Prevention Through Environmental Design (CPTED) .............................. 7
Cyber Crime ................................................................................................. 8
Employee Theft ............................................................................................ 9
Online Crime Mapping .................................................................................. 10
Robbery ......................................................................................................... 11
Shoplifting ..................................................................................................... 12
Workplace Violence ...................................................................................... 13
Business Watch Resources ........................................................................... back cover

Protect your place of business.
Let’s get started on learning how!
What steps are you taking to protect the people, money, inventory, private records and legal documents in your place of business?

Crime prevention is an important element for a successful business. It is essential to reducing loss. It can also help you attract and keep customers by creating a perception of safety in and around your business.

Take the time to assess the vulnerability of your business to all types of crime. Consider the physical layout, employee hiring and training practices, and overall security measures. Learn how to respond quickly and effectively to suspicious or criminal activity and train your employees to do so.

**Crime Prevention Through Environmental Design**

Crime Prevention Through Environmental Design (CPTED) is a good starting point. It helps to make your business a defensible space. Implementing CPTED principles does not have to be elaborate or expensive.

CPTED is made up of four key elements:

- **Natural Surveillance.** Is it easy to see into and out of your business, as well as the area around it?
- **Territoriality.** Create the feeling that your business is your space, and criminals don’t belong there.
- **Natural Access Control.** Direct customers to the entrance(s) they should use and discourage or deny access through any other entrance.
- **Maintenance.** Keep your business and surrounding area tidy and clean. This shows there is someone who cares about the location and is watching it.

For more information on CPTED principles, turn to Page 7 of this handbook.

**Employees**

Choose your employees very carefully. Pre-employment background checks are a good business practice. Also take the time to check references provided by applicants, especially those of former employers or supervisors. For more on good hiring and management practices, turn to Page 9 of this handbook.

**Harden the Target**

Install the highest quality doors, windows, locks and safe you can afford. Alarm and camera systems are a good investment. Consider the cost of each security improvement against the potential savings through loss reduction and lower insurance premiums.
Good Recordkeeping

Keep detailed, up-to-date business records, such as inventories and banking records. Record serial numbers from computers and other equipment, along with item name, make, model, purchase cost and year. For items without serial numbers, engrave with a personalized identification number (not your Social Security number). Put Operation ID stickers near perimeter doors and windows to let criminals know your property is documented. Store back-up copies in another location.

Report Crime and Suspicious Activity

If you see suspicious activity or a crime occurs, call 9-1-1 immediately.

It’s imperative that you and your employees learn to be good witnesses and to observe important details. Key features to note are sex, race, height, weight, approximate age, hair color, eye color, clothing, and any scars, marks or tattoos. Write the information down as soon as possible can after an incident.

Being able to provide law enforcement with an accurate vehicle description can make the difference between a criminal getting away or being apprehended. License plate numbers, even partial numbers, are of tremendous value. Along with vehicle color, try to use detailed descriptions when identifying a suspect vehicle to police:

- Kind—car, truck, motorcycle, SUV, van
- Make and model—e.g., Ford Explorer, Toyota Tundra, Volkswagen Jetta
- Other—identifying bumper stickers, dents, detailing, company logos, etc.

Be Aware of Crime In Your Area

The Snohomish County Sheriff’s Office maintains an online crime mapping tool. This tool allows you to specify an address and time frame, and to select the type of crime activity you want to see mapped on the image. You also can sign up to receive free e-mail alerts when crime occurs in your area. For more information on crime mapping, turn to Page 10.
Burglary

Commercial burglaries are often crimes of opportunity that occur after your business closes. If your business is well secured, unauthorized entry is made difficult, time-consuming, noisy and visible.

First, consider how your property looks from the burglar’s view. Every opening represents a potential security breach and should be inspected. Update or install locks, lighting, alarms and cameras. Illuminate all entry points. Use low-watt lights inside and bright lights outside.

Second, establish a closing routine or check list to make sure employees lock doors, windows and set the alarm. Build a rapport with nearby business owners to discuss problems or nuisances and then identify solutions that benefit everyone.

### Doors and Windows

- Secure doors and windows with high quality locks. Double cylinder, dead-bolt locks with one inch throw bolts are preferred for doors.
- Install cylinder guards and strike plates to slow down forced entry and prevent “jimmying.”
- Use heavy-duty solid construction for rear doors, with bars and u-brackets secured to the structure for added strength.
- Install burglar-resistant glass, wire mesh or iron bars on windows.
- Padlocks should be made of case hardened steel, mounted on bolted hasps.

### Alarms and Cameras

- Take the time to research alarm and camera systems to learn what fits your specific needs and budget. For more consumer tips, visit the Electronic Security Association of Washington website at www.waesa.org.
- Remember, alarms are an entry detection and notification tool—not a physical barrier.
- Have a professional install your alarm and/or camera system. Ask if they do pre-employment screening of their employees.
- Have clearly visible alarm and camera surveillance signage.
- Test your system regularly.
- For a camera to be useful to law enforcement, it needs to provide good facial recognition or vehicle detail. Carefully consider camera quality and placement.
Check Fraud/Counterfeit Money

If your business accepts personal checks, establish a detailed check acceptance policy to help identify and avoid bad checks. Don’t just make a document and file it away—be sure to train your employees on the new policies and post reminders in visible and prominent locations.

Trust your instincts and be on the lookout for suspicious behavior or fraud “red flags.” For questionable transactions, call the customer’s bank to verify legitimacy of a check.

Check fraud

Common check policies include variations of these guidelines:

- Checks must be from a local or in-state bank.
- Checks should not be written and accepted for more than the purchase amount.
- Checks should not be accepted that are unnumbered or non-personalized checks.
- Accepted checks should be deposited as quickly as possible.
- Collect a returned check processing fee.

Instruct your employees to carefully examine every personal check for information:

- **Personalization:** The customer’s complete name and address must appear on the check.
- **Date:** The check date must be current. Do not accept post- or future-dated checks.
- **Bank I.D. numbers:** The check must have a bank identification number, or routing transit number, that runs across the bottom, along with the customer’s account number and check number.
- **The “Pay to the Order of” section:** must indicate your business’s name.
- **Dollar amounts:** Both the written and numeric amounts must match.
- **Signature:** The check should be signed in your presence and signature verified with photo identification. Also verify that any physical description on the identification matches the person presenting the check.

Counterfeit money detection

Be alert for counterfeit money. If it looks suspicious, compare it to a genuine bill. Pay attention to the feel of the paper and details in the printing. All genuine bills have tiny red and blue fibers embedded in the paper; counterfeiters sometimes try to reproduce these by printing them on the paper. Examine the serial numbers to make sure that they all match and are evenly spaced. Look for a security thread running from top to bottom.

Keep a counterfeit detection pen near your cash register. These inexpensive pens contain an iodine solution that creates a black mark on counterfeit bills. When applied to a genuine bill, no discoloration occurs.

For more information on how to detect counterfeit money, and what to do if you receive a counterfeit, visit [www.secretservice.gov/know_your_money.shtml](http://www.secretservice.gov/know_your_money.shtml).
Crime Prevention through Environmental Design (CPTED) is made up of four key elements:

### Natural Surveillance

Is it easy to see into and out of your business, as well as the area around it? Natural surveillance can be enhanced by:

- Clear visibility from inside the business to the street, sidewalk and parking areas.
- Window signs covering no more than 10 percent of window space.
- Interior shelving and displays no higher than five feet.
- Well lit exterior and parking lots.
- No hiding places in loading areas.
- All entrances easily viewed by employees.

### Territoriality

Create the feeling that your business is your space, and criminals don’t belong there.

A business can declare its territory by:

- Property lines and private areas defined by plantings, pavement treatments, short walls or fences.
- Business well identified by signs, including for those parking in the rear.
- Reception and cash register areas positioned to screen all people entering.
- Parking areas clearly marked and separated from pedestrian walkways.

### Natural Access Control

Direct customers to the entrance(s) they should use and discourage or deny access through any other entrance. Access control can be accomplished by:

- Walkways and landscaping that direct visitors to the proper entrance and away from private areas.
- No easy access to the roof.
- Exterior doors hinged on the inside, with a dead bolt lock.
- All windows with locks.
- Detached storage sheds or other buildings with lockable windows and doors.

### Maintenance

Keep your business and surrounding area tidy and clean. This shows there is someone who cares about the location and is watching it.

Maintenance should include:

- Structures painted and in good repair.
- Weeds abated; trees and bushes trimmed.
- All lighting fixtures in good operating condition.
- Litter removed from surrounding area.
- Graffiti removed promptly.
Cyber Crime

Small businesses become increasingly vulnerable to cyber crime as they rely on new technologies to stay competitive. Financial loss from cyber crime can be very high. Equally damaging is the loss of reputation if you must inform your customers that their personal information has been compromised.

There are steps you can take to shield your business from cyber attack. As you take needed technological steps to prevent cyber crime, you also need to educate your employees about potential threats. They are your first line of defense against cyber crime.

A few basic steps that every business should take to minimize risk:

- Analyze your online and operating systems to determine areas most at risk.
- Install anti-virus and other security software, and update them frequently.
- Change passwords regularly, and don’t use the same password for all your accounts.
- Back up critical information and encrypt any sensitive data about the company or customers.
- Consider using a dedicated computer for online financial transactions, independent of more general Internet activities.
- Educate your employees about company-specific security procedures as well as overall best practices.
- Implement a security agreement, signed by all employees, to emphasize their role in maintaining a secure online environment.

The Federal Communications Commission has created a Small Biz Cyber Planner, a tool for small businesses to create customized cyber security planning guides. The Cyber Planner may be found online at www.fcc.gov/cyberplanner.
Employee Theft and Fraud

Employee theft and fraud can be a serious problem for business owners. According to the U.S Small Business Administration, occupational fraud results in the loss of roughly 5 percent of an organization’s annual revenue.

1. The first step to preventing fraudulent employee behavior is to make good hiring decisions. Pre-employment background checks are essential, especially for those employees who will be handling cash, high-value merchandise, or have access to sensitive customer or financial data. For more information on the types of information you may wish to consult as part of a pre-employment check, visit www.sba.gov/content/pre-employment-background-checks. To request a criminal background check, visit https://fortress.wa.gov/wsp/watch.

Also take the time to check out references provided by applicants, especially those of former employers or supervisors.

2. Create an employee code of ethics and conduct. Make it part of new employee orientation, and review it annually with all employees. Establish and enforce clear policies about employee theft, substance abuse, security procedures, and reporting crime. For ideas on how to develop an employee policy manual, visit www.sba.gov/content/employee-handbooks. Reward employees who discover and report security problems.

3. Maintain strong internal controls over the movement of cash and goods in your business. Identify high risk areas for your business and audit for violations on a periodic basis. Reconcile bank statements, cash, and sales reports frequently, and treat unusual transactions with suspicion. Keep an accurate inventory system and check it regularly.

4. Develop a key control policy. You may be vulnerable if you are unsure who has access to your building. Make sure the keys to your business cannot be duplicated without your permission. Document the names of employees who have company keys.

The security cameras you install to deter robbery and burglary can also help detect employee theft. Monitor business activity and income patterns over time to see if income drops during any particular shift or situation.
Online Crime Mapping

The Snohomish County Sheriff’s Office maintains an online crime mapping tool. This tool allows you to specify an address and time frame and choose the type of crime activity you want to see mapped on the image. Checking the map and signing up for e-mail alerts can help you be aware of what’s happening in your area so you can pass the information on to employees and be more alert to particular types of crime.

1. To access the Snohomish County Crime Mapping page, select the blue icon on the Sheriff’s Office home page (http://sheriff.snoco.org). Next click “Take me to CrimeMapping.com!”

2. From the CrimeMapping.com home page, in the white box at the top, enter the address you wish to search. For example: 4809 132nd St. SE, Everett, WA. Then click the green “Search” button on the right.

   The map will automatically select a one-mile radius around the address you entered. You can adjust the size of the radius or choose to eliminate it by clicking on “Remove Radius.”

3. Use the “Crime Types” menu to select the crimes you’re interested in. The “Check All” button is a good shortcut if you want all crimes mapped. To help you understand what the various crime icons mean, hover over each symbol for a description.

4. Specify the time period you want to search using the “Dates” tab. Select start and end dates for your search, then click the “Apply” button on the right. Crime information is available for the past 180 days.

5. To collapse the menu bar for a better view of the map, click the blue arrow on the right side of the menu bar.

6. Left-click on a crime icon for more details. A box will open that includes date of the crime, which block it occurred in, and a brief description. From this box you can also link to the Sheriff’s Office Web site for crime prevention tips or to locate registered sex offenders.

7. If you wish to receive free e-mail alerts when crime occurs in your area, click on the orange “Receive Crime Alerts” in the upper right corner.

8. To learn about more of the great features of this tool—such as sharing the map you’ve created with others, displaying a detailed list of the crimes on your map, or making colorful charts—click “Help” at the top of the page.
Robbery

Robbery is a frightening and potentially dangerous situation. Keep in mind that money and property can be replaced, and are not worth risking your life to protect. You can dissuade potential robbers by minimizing temptation and maximizing their chances of being caught.

**Before a Robbery**
- Greet everyone who enters your business.
- Keep doors and windows clear of signs and posters, to allow good two-way visibility.
- Place a surveillance camera behind the cash register facing the front counter.
- Install height-appropriate outside cameras for good coverage up and down the street.
- Install a robbery alarm.
- Make bank deposits at least once a day.
- Keep a clean, well-lit business, inside and out.

**During a Robbery**
- Do as instructed; stay calm and don’t resist.
- Don’t make any sudden moves and keep your hands in sight.
- Get a look at the robber but don’t stare.
- Notice the robber’s voice, or any odd mannerisms.
- Activate the panic alarm ONLY when it’s safe.
- If safe, get a description of the robber’s vehicle and direction of travel.
- Don’t chase or follow the robber out of your place of business.

**After a Robbery**
- Close the business and lock the doors.
- Call 911, even if the alarm was activated.
- Preserve evidence—don’t touch anything the robber may have touched.
- Ask witnesses to stay until the police arrive.
- To maintain the integrity of the police investigation, don’t talk about the incident until a police officer takes your statement.
- Only step outside when the police arrive and contact you.
- Call your business owner, manager or other designated person.
All retailers are susceptible to shoplifting, no matter how big or small the business. Shoplifters may work in groups of two or more to distract the sales staff while they pilfer. Shoplifters learn to take advantage of busy stores during peak hours or they may hit at times when employees are less alert, such as opening, closing, and shift change.

Hiding merchandise is the most common method. Items are concealed in clothing, handbags, strollers, umbrellas or inside purchased merchandise. Bold shoplifters may grab an item and run out of the store. Other methods include price label switching, short changing the cashier, and phony returns.

“Red Flag” Signals.
There is no typical profile of a shoplifter. However, there are some signs that should signal a red flag for retailers. Keep a close eye on shoppers who:

- Spend more time watching the cashier or sales clerk than actually shopping.
- Wear bulky clothing during warm weather, or coats when unnecessary.
- Walk with short or unnatural steps, which may indicate they are concealing lifted items.
- Take several items into the dressing room and leave with one item.
- Seem nervous or pick up random items with no interest.
- Enter the store as a large group, especially juveniles. A member of the group causes a disturbance to distract sales staff.

How to Combat Shoplifting.
Retailers can use store layout, customer service techniques, and common security practices to combat shoplifting:

- Greet every customer that enters the store. Let them know you are aware of their presence.
- Schedule an adequate number of employees to work at one time.
- Design the store layout so customers must pass by the register area and staff to exit the store.
- Approach suspicious shoppers and ask if they need assistance. Make them feel watched.
- Do not display merchandise near the exits.
- Keep small, expensive items in locked cabinets or behind the counter.
- Keep dressing rooms locked and limit the number of items taken in by each customer.
- Never leave the cash register unlocked or unattended.
- Require receipts for refunds for cash. Trash any discarded receipts immediately.
- Don’t allow customers to distract the cashier while another person is being checked out.
- Every bag should be stapled shut, with the sale receipt attached.
- Cashiers should watch price tags and be on the lookout for price switching.
- Look inside boxes and other products to be sure they don’t contain lifted items.
- Post ‘Shoplifters Will Be Prosecuted’ signs in clearly visible locations.
Workplace Violence

The term “workplace violence” covers a broad spectrum of behaviors. It includes aggressive behaviors that disrupt the flow of work and cause employees to be concerned for their personal safety, such as bullying, stalking, and threatening. The more lethal end of the spectrum consists of overt violence causing physical harm or death, with or without weapons.

Workforce violence falls into four general categories:

1. Incidents that involve perpetrators with no personal relationship to the victim or business.
2. Incidents that involve perpetrators who currently receive services from the business (such as retail, health, or service-industry settings).
3. Incidents that involve current or former employees acting out against their present or past places of employment.
4. Domestic disputes between an employee and the perpetrator that spill over into the workplace.

Workplace violence can strike anywhere. The best protection an employer can offer is to establish a zero-tolerance policy toward workplace violence against or by their employees, and include that information in new employee orientation. Encourage employees to report and log all incidents and threats of workplace violence.

Provide safety education for employees so they know what conduct is not acceptable, what to do if they witness or are subjected to workplace violence, and how to protect themselves. There are steps you and your employees can take to de-escalate potentially violent situations:

- Stay calm and listen—encourage dialogue.
- Acknowledge feelings to indicate you know they are upset.
- Use delaying tactics to give the person time to calm down.
- Accept criticism and ask clarifying questions.
- Point out choices and reassure everything will be OK.
- Try to keep a physical barrier, such as a desk or chair, between you and the aggressor.
- Do not get blocked from the exit.
- Do not physically contact the other person, or make sudden movements.
- Do not accept demands from the aggressor or attempt to bargain.
- Do not challenge, belittle or threaten the individual.
- Do not take sides, or agree with distortions.
- Do not make false statements or promises you cannot keep.

Be very alert to signs of escalating aggression. If a person’s behavior escalates beyond a reasonable level or they become physical, disengage and immediately call 9-1-1.

The Occupational Safety and Health Administration (OSHA) provides many safety and health programs to assistance businesses. For a copy of their Workplace Violence Fact Sheet, and other useful publications, visit www.osha.gov/pls/publications/publication.html.
Business Watch Resources

Snohomish County Sheriff’s Office
crimeprevention@snoco.org
http://sheriff.snoco.org

Business Watch Signs
www.nnwi.org/business_products.asp

Federal Bureau of Investigation
Seattle Field Office
www.fbi.gov/seattle

Federal Communications Commission
www.fcc.gov

Federal Trade Commission
www.ftc.gov

Occupational Safety and Health Administration
www.osha.gov

Small Business Administration
www.sba.gov

Snohomish County Business Watch
www.TheSCBW.org

U.S. Secret Service
www.secretservice.gov

Washington Labor & Industries
Small Business Center
http://www.lni.wa.gov/Main/smallbusiness/

Washington State Attorney General
www.atg.wa.gov

Washington State Patrol
Criminal Background Checks
https://fortress.wa.gov/wsp/watch/

March 2013