Retail Council of Canada
www.retailcouncil.org

www.rbc.com

RETAIL BUSINESS SECURITY SELF ASSESSMENT

Though we all wish it were not so, the fact is theft and fraud are issues that retailers across Canada must wrestle with every day.

A recent poll of independent retailers conducted by Ipsos Reid on behalf of Retail Council of Canada and RBC confirms this, with 87 per cent of Canada's small and medium-sized retail business owners reporting they have been victimized by retail crime within the past year.

It's an unfortunate reality, but one that must be dealt with in order to promote a prosperous business climate for the thousands of retailers that make up our industry.

Retail Council of Canada has long been an advocate for retailers on the loss prevention front, campaigning on behalf of retailers who want to move beyond just talking about loss prevention to doing something about it.

That is why Retail Council of Canada is proud to collaborate with RBC in presenting these best practices, developed with the independent retailer in mind. Retailers have told us about the loss prevention issues that matter most to them, and it is our hope that the following pages will better prepare those retailers and help prevent future incidents involving their people and their property.

If you are a member of Retail Council of Canada, thank you for your continued support. If not, we have a number of other loss prevention publications and programs to assist you in growing your business. They are just a few of the tools available to our members, and I encourage you to visit www.retailcouncil.org to find out more.

Sincerely,

Bill Yetman
Executive Vice-President,
Retail Council of Canada

RBC is delighted to collaborate with the Retail Council of Canada to produce this new loss prevention handbook for independent retailers. No matter the size of your business, we know you will find the information contained in this guide to be of tremendous value to you and your staff.

Your business is part of a dynamic industry that's constantly evolving in response to a changing marketplace. At RBC®, we understand the demands of your business environment, which is why we have a national network of account managers who specialize in serving the needs of retailers.

Our retail specialists understand the sophistication of today's consumer. And they understand the changing trends, opportunities and challenges you face. As your business grows and changes, an RBC Retail Specialist account manager can help you achieve your goals by providing you with the right financial advice and solutions at the right time. This Loss Prevention handbook is just an example of one of the many ways we can help businesses like yours.

For more information on RBC and how we might be able to help your business, please visit us at www.rbcroyalbank.com/retail.

Stephen Aikman
National Manager, Retail and Service Clients
RBC Royal Bank

INDEX

DISCLAIMER

The content of this publication is of a general nature and is not intended to address the circumstances of any particular individual or organization. Although we endeavour to provide accurate and timely information, errors and omissions may occur. Readers should not act on such information without appropriate professional advice after a thorough examination of the circumstances of the particular situation.

THEFT BY EMPLOYEES

Theft by staff is an unfortunate aspect of managing and owning a retail outlet. Staff can steal in a number of ways: directly, by stealing revenue, stock, other employees' or clients' property; or indirectly, by helping other people steal.

PREVENTION

1. Screen all applications for employment carefully. Check references provided and ensure applicants explain any gaps in past employment. Include credit and criminal checks when appropriate.
2. Consider using ongoing and regular criminal history checks.
3. Develop policies that clearly identify system processes, define acceptable behaviours and determine consequences for policy breaches.
4. Develop an orientation program for new employees that provides a clear explanation of policies and procedures.
5. Identify the preferred policy for how employees and friends and families of employees purchase goods from the business and communicate this policy to all staff.
6. Adopt a "prosecution policy" for dealing with employee theft. Ensure staff members understand the policy. A successful, widely publicized prosecution can act as an effective deterrent for others.
7. Ensure employees know that management tracks and logs employees' online activity. Ensure that staff cannot tamper with online logs. Review logs regularly for unauthorized or unusual activity.
8. Be aware of employees' actions related to online activity, cash handling, and confidential paper-based information (e.g., credit cards), particularly employees who receive less than favourable reviews or do not receive an expected promotion.
9. Provide strong and consistent supervision of all staff. Deal with issues of concern, such as shortfalls in daily takings, immediately.
10. Provide ongoing retail security training to all staff.
11. Within limits, encourage employees to contribute to retail security initiatives.
12. Have an effective asset inventory control system to identify losses as they occur.
13. Provide a designated area where staff can lock their belongings.
14. Maintain strict control of store keys and codes at all times to ensure internal security.
15. Regularly inspect dispatch and delivery areas to guard against falsification of records, theft or collusion between drivers and staff.
16. Watch for customers who continually return to the same register or the same staff member.
17. Recognize and reward staff loyalty and honourable behaviour.
18. Write a Code of Conduct to educate employees about acceptable behaviour.

RCC the voice of retail
Retail Council of Canada
www.retailcouncil.org

RBC
www.rbc.com

AGGRESSIVE PEOPLE

While the vast majority of customers are polite and friendly to deal with, violent outbursts that occur inside a store or small business can result in physical injury to staff, customers, the offender and/or damage to stock and fixtures.

It may be useful to keep photocopies of the Description Form (page 8) in a predetermined, convenient location within your business for quick and easy reference and use by staff. Make sure that staff members are familiar with its location and use.

PREVENTION

Educating staff about conflict resolution can be a useful investment in avoiding customer complaints and potential risks such as those outlined above. Staff should be skilled in differentiating between assertive and aggressive customers and potentially violent customers.

In all instances of dealing with aggressive people, the main priority is to ensure the safety of yourself, your staff and your customers. Every situation is different and there is no one absolute set of procedures for dealing with aggressive people. Following some basic steps, however, may assist staff in responding to such situations.

BASIC SECURITY TIPS

1. Assess the situation and remain calm at all times.
2. If store security officers are employed, ensure staff are aware of when and how to contact them.
3. If it appears that the safety of staff or customers is at risk, telephone the police immediately.
4. Do not respond to the customer's bad behaviour in the same manner.
5. Remain respectful. Try to restore a sense of justice for the person. Explain what options are available and encourage them to try one of these.
6. Patience is usually a good strategy. This can be achieved by not only listening to the person but by acknowledging their problem or situation:
   - Staff members should not take insults personally, as they are being delivered by a person who appears unreasonable and may relate to business policies and procedures, not the employee.
   - Listening can be useful in allowing the person to "let off steam."
   - Remember that anger diminishes with time.
7. Staff not involved in the incident should not become an audience; however, they should monitor the situation for any possible escalation.
8. If the person is not able to be calmed and they continue to be offensive or obnoxious, politely request that the person leave the store.
9. If a person refuses to leave after a polite request, contact the police and await their arrival. Do not engage in any further unnecessary dialogue.

VIOLENT OFFENDERS

1. Do not enter the person's physical space, as this can escalate the situation.
2. Discretely remove any items that could be used as weapons.
3. Counter areas or display stands can be discretely used to create natural barriers and distance between staff members and the other person.
4. Employees are entitled to protect themselves from violence, but the amount of force used must be reasonable and proportionate to the threat. Excessive defensive force is not justified and can result in a counter claim of criminal assault or civil litigation.

RCC the voice of retail
Retail Council of Canada
www.retailcouncil.org

RBC
www.rbc.com

ARMED ROBBERY

A small amount of planning will reduce the risks of armed robbery to your business, thereby maximizing the safety of your employees and customers.

It may be useful to keep photocopies of the Description Form (page 8) in a predetermined, convenient location within your business for quick and easy use by staff. Ensure staff members are familiar with its location and use.

The aim of preventing armed robberies should be to:

- prevent the business being targeted by offenders
- maximize the safety of employees and customers
- reduce the impact of the crime on your business
- assist police in the apprehension process of any offender(s)

PREVENTION

1 Be alert to strangers or individuals who may be observing your business or who are asking questions about how the business runs.

2 Ensure all back and side doors and windows are kept secure.

3 Do not discuss cash holdings or movements of cash in public.

4 Consider installation of a safe in a secure area but within close proximity to the cash register. The safe should be secured to a sturdy fixture.

5 Reduce cash held at counters to a workable minimum.

6 Predetermine and designate escape routes and safe areas for employees to move to when required.

7 Ensure that staff members are aware of security and armed robbery procedures and know what to do in the case of such an event. This routine should be regularly practiced as with any other type of emergency drill.

8 Make use of signage and stickers both inside and outside your business promoting such security measures as time-delay locks, video surveillance and minimum cash held on premises.

9 Consider installation of electronic methods of payment to reduce the amount of cash kept on hand.

10 Consider the installation of additional security devices such as quality Closed Circuit Television (CCTV).

RCC the voice of retail
Retail Council of Canada
www.retailcouncil.org

RBC
www.rbc.com

IN THE EVENT OF AN ARMED ROBBERY

1. Try to remain calm, assess the situation and do exactly as the offender says. Remember: the No. 1 priority is your safety, the safety of other staff and the safety of your customers.
2. Activate alarm devices as soon as possible, but only if it is safe to do so.
3. Avoid sudden actions and calmly explain any necessary movements to the offender. These could pose an unintended threat to the offender, who may already be anxious and tense.
4. Speak only when spoken to as any conversation with the offender will prolong the incident.
5. Unless otherwise ordered, discretely watch the offender(s). Make a mental note of their description, especially scars, tattoos, and other prominent or distinguishing features.
6. Avoid direct eye contact with the offender(s).
7. Take note of the offender's conversation, including any indecent language, accent, nicknames or speech impediments.
8. Observe and take note of any weapons that are being used.
9. If safe to do so, observe the direction of travel taken by the offender(s) when they leave the premises.
10. If safe to do so, look to see if a vehicle has been used and if there are any other occupants; record the licence plate number, make, model and colour of the car.
11. Never take drastic action during the robbery and do not chase the offender.

AFTER THE ROBBERY

1. Immediately call 911 and provide the operator with:
   - Exact location – business name/address of where the crime occurred, including the closest intersecting street
   - Your name
   - Details of persons injured and whether medical assistance is required
   - Date/time/nature of offence
   - Number and description of offender(s), including any vehicles used
   - Direction of travel
2. Only hang up the telephone when told to do so and stay off the phone until police arrive unless you remember additional information that may be important.
3. Close the premises to the public and keep unauthorized persons out.
4. Make sure that no person touches or moves any items where the offender(s) was/were present.
5. Consider arranging for someone to meet the police outside, particularly in large shopping areas, to make the response time more efficient.
6. Request that witnesses and customers remain until the police arrive. Failing that, request their names, addresses and telephone numbers and pass them on to police when they arrive.
7. Make sure witnesses are isolated from each other or are aware not to discuss descriptions of what happened with other witnesses.
8. Witnesses should independently try to write a full description of offender(s) and what actually occurred in as much detail as possible.
9. Do not make any statements to the media before discussing the matter with police.
10. Supply to police all details, no matter how insignificant they appear to you. This could include earlier suspicious customers; rude, drunk or drug-affected customers; or simply details of certain cars constantly driving past.
11. Crime affects different people in different ways and the impact may not be felt immediately. Consideration should be given to organizing professional trauma counselling for employees affected by the crime.

RCC the voice of retail
Retail Council of Canada
www.retailcouncil.org

RBC
www.rbc.com

IN CASE OF ROBBERY

NOTIFY POLICE AND FILL IN THE BLANKS.

SEX (CIRCLE)

RACE
AGE
HEIGHT
WEIGHT
HAIR
HAT TYPE
EYES
TIE
GLASSES TYPE
COAT
TATTOOS
SHIRT
SCARS/MARKS
TROUSERS
COMPLEXION
SHOES

BAIT MONEY SERIAL NUMBER	AUTOMOBILE DESCRIPTION (LICENSE NUMBER, MAKE, COLOUR)

WHAT ROBBER SAID

LONG BARREL REVOLVER	SNUB NOSE REVOLVER	SAWED-OFF RIFLES
		Bolt-action  Lever 
LARGE AUTOMATIC	**SMALL AUTOMATIC**	**SAWED-OFF SHOTGUNS**
		Pump  Automatic  Single Shot 

CASH HANDLING

The safe handling of cash, which incorporates the secure storage and transport of cash, can help prevent crimes. All staff members responsible for cash must know safe cash handling procedures.

SOME CONSIDERATIONS RELATED TO CASH ON PREMISES

1. Advertise that you keep a minimum amount of cash on the premises.
2. Consider installing a safe in a locked room away from public view. Ensure the safe is securely fitted to a solid, non-removable object.
3. Before you count the cash, ensure the attending staff member is out of public view in a safe and secure area of the business. This may include checking the premises, including washrooms and other concealment locations, for people who may be hiding.
4. Secure all exterior doors and windows from the inside before counting money.
5. If cash is counted in a specific area, consider installing a telephone or duress (panic button) alarm system in that location.
6. Don't discuss cash amounts or handling procedures in public.
7. It is unadvisable to take cash home and be known to do so.
8. To minimize damage to cash registers by after-hours thieves, consider leaving your tills empty and open overnight.

CASH REGISTER SECURITY IS CRITICAL

1. Do not leave the register drawers open longer than necessary during business hours.
2. Position the register to eliminate or restrict public view of its contents, which should not be within the reach of potential offenders.
3. Keep as little cash in the register as possible by regularly transferring it to a more secure place. Ensure this is done at random times throughout the day.
4. Ensure staff members do not keep large amounts of cash in their pockets while serving.
5. Encourage staff vigilance.
6. Create a store policy that limits cash-back requests. A sound policy requires customer signatures for cash-backs, limits how much a customer can request and records the cash register transaction code.

TRANSPORTING CASH TO THE BANK

- For business owners, employee safety is paramount. Use a cash transport service, especially when large amounts of monies are involved.
- If you use employees to courier deposits, check employees' references and criminal records. Couriers should be able-bodied, properly trained in cash carriage procedures and robbery response, feel comfortable with the duty and have access to a mobile telephone.
- When employees transport cash, ensure that company uniforms are not worn. If they are worn, employees should cover uniforms with other clothing items. Any badges should be removed from uniforms that could identify the courier as store staff.
- Use plain, non-descript bags for carrying cash. Do not place money, cheques and other valuables into a handbag, bank bag or parcel that identifies the store.
- Vary the route and times of bank deposit trips. Do not follow a pattern.
- Be alert at all times to persons and vehicles that follow you. If you are followed, note the registration and record a description of the person.
- Watch for suspicious persons and vehicles, and use 911 to report observations (including descriptions) to the police.

STAFF TRAINING

1. All staff involved in cash handling should be regularly trained in correct cash handling techniques.
2. All office staff, including those not involved in cash handling, should be regularly trained in the procedures to be followed in the event of a robbery.

RCC the voice of retail
Retail Council of Canada
www.retailcouncil.org

www.bankofcanada.ca

RBC
www.rbc.com

CREDIT CARD FRAUD

With customers using credit cards more often for their purchases, credit card fraud is on the rise. Educating front-line staff is key to preventing credit card fraud.

CUSTOMER CONSIDERATIONS

Be alert for customers who act in an unusual manner:

- Are they hurried, nervous, blushing, hesitant or overly chatty or friendly?
- Do they make a purchase without regard to price, quality or size? For example, do they buy several items of clothing in the same style, but not in the same size?
- Do they appear anxious to complete the sale and leave the premises with their purchase?
- Do they repeatedly return to make additional charges?
- Do they bring the card straight out of a pocket instead of from a wallet?
- Do they produce a card with a name that does not match the customer? For example, does a man try to use a card with a woman's name?
- Are they reluctant to produce photo identification?
- Do they order goods over the telephone and then advise that they are elsewhere but will send a friend to collect the goods? This allows the offenders to avoid producing the card that may be stolen.
- Do they buy merchandise randomly prior to store closing? Do they buy clothes without trying them on? Do they purchase electronics or other expensive items quickly?

CARD CONSIDERATIONS

When you get the card, look at the front and check to determine if:

- the card has a valid expiry date
- the card is damaged
- the embossing has not been altered
- the hologram looks authentic
- the card is listed on the warning bulletin

MAIL ORDER/TELEPHONE ORDER (MOTO) AND INTERNET FRAUD

There is anonymity buying through the mail, over the telephone or online, but watching for the following can help reduce the risk:

Do customers order big-ticket items for resale?

- Do customers ship orders "Rush" or "Overnight" for a quick sale?
- Are there transactions on similar account numbers?
- Are there orders shipped to a single address but made from multiple cards?
- Do customers order multiple copies of the same item?
- Do customers use multiple cards to pay for a single purchase?
- Do customers have orders shipped to another country other than the country of the cardholder?

As a general rule:

- Never accept orders via e-mail. This exposes card data.
- Be aware of larger-than-normal purchases. Criminals try to maximize their purchases.

Remember: an authorization for a transaction doesn't necessarily mean that it is the real cardholder or a real card plastic that is being used. It means that the card number has credit available and is not blocked.

SIGNATURE CHECKS

When you check the signature, ask:

- Has the card been signed?
- Has the signature area been altered?
- Do the signatures match?

RCC the voice of retail
Retail Council of Canada
www.retailcouncil.org

RBC
www.rbc.com

SECURITY FEATURES OF CREDIT CARDS

- Card numbers should be clear and uniform in size and spacing.
- The last four numbers of the card should be embossed in the hologram.
- The expiry date should be current.
- The number on the card is always the same as the number on the sales draft that is printed.
- The signature panel on the back should be followed by a three-digit card verification validation (CVV).

PIN PAD PROTECTION

- Ensure your terminal is installed so that your customers can shield their PIN.
- Check PIN pad devices frequently to ensure they have not been altered. Skimming devices can be sophisticated and can be attached to PIN pad devices inconspicuously.
- Random visits to the store by a manager will help reduce fraudulent activity with PIN pad devices by employees.
- Check for suspicious holes in the ceiling and walls where cameras might be placed.

BASIC SECURITY TIPS

1. If using an electronic terminal, ensure printed receipts match with the printed details on the card.
2. Do not return the card to the purchaser before the sale has been processed and the signature confirmed.
3. If you use a manual imprint system, ensure the carbon sheets are destroyed.
4. Should alterations or irregularities be found:
   - hold on to the card
   - ask for additional photo identification
   - call for authorization or contact the credit card provider
5. If the transaction is not authorized:
   - hold on to the card
   - listen to the instructions given to you from the payment processing operator
   - call the police if required
6. Contact the bank card authorization centre to obtain authorization for credit card transactions:
   - when the value of the transaction exceeds the floor limit
   - when you suspect that the card presenter is not the cardholder
7. Ensure staff members are trained on card acceptance policies and procedures, including the ability to identify fraudulent credit cards, cheques and currency.

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Any merchant or service provider that stores, transmits or processes credit card information must adhere to the Payment Card Industry Data Security Standards to ensure cardholder data is adequately safeguarded.

This standard is the result of a collaboration between the major credit card companies and is designed to create common industry security requirements. Contact your acquirer or credit card company for further information on the 12 basic requirements and obtaining certification.

For additional advice about credit cards, refer to the Web sites of banking institutions or credit card associations:

Interac Association
(416) 362-8550, www.interac.ca/merchants/home.php

Industry Canada - Office of Consumer Affairs
www.ic.gc.ca/epic/site/oca-bc.nsf/en/h_ca02306e.html

MasterCard International - Canada Region
www.mastercard.com/ca/merchant/en/security/index.html

Visa Canada Association
www.visa.ca/en/merchant/

RCC the voice of retail
Retail Council of Canada
www.retailcouncil.org

RBC
www.rbc.com

ELECTRONIC CRIME (E-CRIME)

Increasingly, small business retailers are opening their business and telephone lines to customers and suppliers through electronic transactions. While these electronic transactions provide many benefits to retailers and customers alike, they can also expose you to unique methods of crime involving your business, suppliers and customers.

HOW CAN I PROTECT MY BUSINESS?

It is important to put in place measures to reduce the risk of e-crimes and protect business information.

BASIC SECURITY TIPS

1. Install reputable anti-virus software and keep it up to date.
2. Install reputable firewall software and keep it up to date.
3. Keep software patches up to date.
4. Passwords should be confidential, complex and changed on a regular basis.
5. Delete without opening any suspicious e-mails – curiosity is a tool often used to hack a computer system or send a virus.
6. Only download software from reputable sources.
7. Back up critical data and keep it separate from your Internet-connected computers. Regularly copy the data to a CD or other backup device.
8. Test that you can recover the information using that backup device.

HOW DO I KNOW IF MY BUSINESS HAS BEEN HACKED?

The following is a useful list of potential indicators that may indicate the presence of hackers:

1. Your website has been changed.
2. Your computer system performance is unusually and exceptionally slow.
3. Secrets of your business have been exposed to the general public or to competitors.
4. Transactions have been changed. For example, a client or supplier account that had a balance of $1,000 now has $950 without your authorization.
5. There is odd activity in a computer log.
6. Established business procedures do not appear to have been followed and transactions are unexplainable. This may indicate that someone is operating outside of your control and using your business.
7. You no longer receive e-mails and no one receives e-mails you have sent.
8. The entire system shuts down.
9. There is a new program on your computer that you didn't install.

ONLINE FRAUD

If you become the victim of online fraud, report the matter to local police. You will need to ensure that you preserve any electronic evidence relating to the matter, including e-mails and any relevant computer logs. If you can, copy this information to a CD or DVD and take it to the police station when you report the matter.

USEFUL REFERRALS

To help you assess the vulnerability of your network, you may want to engage the services of an external independent Internet security organization specializing in "ethical hacking."

RCC the voice of retail
Retail Council of Canada
www.retailcouncil.org

RBC
www.rbc.com

FINANCIAL FRAUD

New methods to defraud businesses, such as cheque fraud, emerge regularly. There are steps you can take to protect your business and help prevent fraud. Efforts on your part can make a significant difference in how often fraudulent activities are prevented.

CHEQUE FRAUD

1. Check with your bank periodically, or when re-ordering your cheque stock, to ensure your cheques contain any new security features that help combat counterfeiting.
2. Always store your cheques, deposit slips, bank statements, and other financial documents in a secure location.
3. Shred cancelled cheques and old statements, or store under the same security as your un-issued cheques.
4. Ensure cheques are held in proper custody during the authorizing or signing process. For example, do not leave a completed cheque with one signature in the "in" box of the person who will countersign; instead, deliver and handle such cheques personally.
5. Reconcile your bank statement daily.
6. Make sure all of the cheques are present when receiving a re-order shipment. Report missing cheques to your bank/cheque supplier immediately. Stolen cheque stock is sometimes mistaken as simply lost, or never sent.
7. Don't leave blank spaces on the payee and amount lines.
8. Use dark ink that can't be easily erased or covered over.
9. Have different accounts for different functions. For example, use one account for payroll, one for accounts payable, one for cheque issuance, and so on. It will be easier to reconcile because only certain transactions will go through each specific account, and other parts of your business can continue without delay if one account needs to be closed.
10. Check with your financial services provider on what fraud prevention services are available.

FRAUD INVOLVING BANKING ACTIVITIES

Separating banking duties by employee is critical to ensure that errors or irregularities are prevented or detected on a timely basis. Here are some examples of some banking duties that should be separated.

The same employee should not:

1. Authorize a transaction and receive and maintain custody of the asset that resulted from the transaction.
2. Receive cheques (payment on account) and approve Accounts Receivable write-offs.
3. Make deposits and reconcile bank statements.
4. Approve time cards and have custody of or issue payroll cheques.
5. Issue cheques and reconcile bank statements.
6. Approve cheques (including calls from the bank or exception reports) and issue cheques or reconcile bank statements.
7. Balance daily receipts and input the data into accounting systems.

RCC the voice of retail
Retail Council of Canada
www.retailcouncil.org

RBC
www.rbc.com

THEFT FROM STORE

Some people refer to store stealing as shoplifting, but no matter what you call it, if someone deliberately takes something from your store that they have not paid for, then it is THEFT.

PREVENTION

STORE LAYOUT & DESIGN

1. Design stores with an open layout that offers good visibility to all areas.
2. Keep shelves and stock neatly stacked and price tags properly secured to goods.
3. Where possible, keep expensive and portable goods locked in cabinets located close to staff working areas.
4. Keep store well lit, particularly around selling points.
5. Warning signs regarding possible consequences of theft and the security measures in place at your store should be clearly displayed.
6. Limit the number of entry and exit points to your store.
7. Ideally, cash registers should be located close to entry and exit points and protected to prevent easy removal of money by offenders.
8. Keep staffrooms and stockrooms locked at all times.
9. Consider installation of surveillance devices, such as surveillance mirrors and Closed Circuit Television (CCTV).

BASIC SECURITY TIPS

1. Acknowledge all customers. Customer service is one of the most effective crime prevention strategies.
2. Pay attention to customers who appear nervous or distracted around merchandise.
3. If you employ store security or loss prevention officers, familiarize staff with their identities and explain how and when security operates and when and how they are to be contacted.
4. Approach people who stand around staff-restricted areas, restrooms, stockrooms or stairways.
5. Be aware of people wearing loose overcoats and bulky clothing, especially in hot weather.
6. Approach and query persons claiming to be tradespersons, particularly in unauthorized areas. Consider requesting to inspect trade-related identification.
7. Be mindful that baby carriages, shopping trolleys, boxes and bags can be used by shoplifters to conceal the goods they are attempting to steal.
8. Count the number of items taken in and out of changing rooms.
9. Ensure empty hangers and excess stock are removed from racks and shelves.
10. Ensure staff are familiar with the items/quantities of stock on display.
11. Keep customers in view at all times and be conscious of having your back to customers.
12. Never leave sales areas or cash registers unattended.

WATCH FOR:

- Hands – they do the stealing.
- Customers who do not appear to have a deliberate purpose to purchase items.
- Customers who remain in the store for lengthy periods of time, or who are “sampling” merchandise that appears inconsistent to customer type.
- Organized distractions that may result in one or more persons attempting to distract staff while another person commits the theft.
- Unsupervised children who are in the store during school hours.

RCC the voice of retail
Retail Council of Canada
www.retailcouncil.org

RBC
www.rbc.com

PERSONAL SAFETY

Under Occupational Health and Safety legislation, all people have the right to work in a safe environment and employers have an obligation to provide a safe working environment. As the name suggests, "personal safety" is a personal matter. An environment or circumstances that enable one person to feel safe may not assist another person's sense of safety. Using some or all of the tips below may assist staff members to satisfy their individual sense of personal safety. But additional factors may need to be considered depending on individual circumstances.

WITHIN THE BUSINESS

1. Familiarize all staff with emergency procedures and policies for dealing with aggressive people, armed robberies, shoplifters, cash handling, etc.
2. Restrict access to employee-only areas and back rooms.
3. Ensure valuables, such as personal possessions belonging to staff, remain locked away at all times. Items such as mobile phones, handbags and wallets should not be left unattended, even for a moment.
4. Install audible door announcers to identify when customers enter the store.
5. Keep doors and windows locked if staff are working late.
6. When a staff member temporarily leaves the premises, notify a second party and advise that person of the staff member's likely movements, expected time of return or arrival at next location.
7. Encourage staff members to move their private vehicles closer to the business during daylight hours. After hours, arrange an escort to the car or have someone watch their safe arrival into the car.
8. Pre-program important numbers such as 911 into business telephones and the mobile telephones of staff members.

IN YOUR CAR

1. Park vehicles as close to your work premises as allowed.
2. Have keys in hand ready for use. Do not search for them in a handbag along the way or when standing at the car door.
3. Check inside the vehicle by looking through the windows before getting in.
4. Consider driving with all of the doors locked and the windows wound up.
5. Do not leave valuable items visible inside the vehicle.
6. When leaving the vehicle, always close the windows, remove the ignition key and lock the doors.

NO AMOUNT OF PROPERTY IS WORTH RISKING YOUR SAFETY

RCC the voice of retail
Retail Council of Canada
www.retailcouncil.org

RBC
www.rbc.com

PRIVACY CONSIDERATIONS

With the rise in identity theft, consumers expect that retailers keep their information confidential. Similarly, you must protect your own private business and financial information to prevent fraudulent activity.

PRIVACY POLICIES

1 Review your employee practices. Research shows that the "insider threat" is real and a significant factor in privacy breaches. Train employees on your privacy and information security program. Success of the overall privacy program requires responsible owners and engaged employees.

2 In addition to other business response plans, maintain a Privacy Breach Response Plan. This should include an assessment of the incident and containment, an evaluation of the risks associated with the breach, consideration about whether you will notify clients and regulators and whether you require preventive measures to prevent a recurrence. The Office of the Privacy Commissioner of Canada has published "Key Steps for Organizations in Responding to Privacy Breaches" to help businesses: **www.privcom.gc.ca/information/guide/2007/gl_070801_02_e.asp**

3 Develop a formal written privacy policy detailing the organizational policies and practices relating to the management of client and employee personal information.

4 Be open about your privacy practices. Tell employees and customers how you collect and use personal information, describe the type of information you collect, and explain your disclosure practices and consent provisions. Review your privacy policies regularly and keep them current.

5 Appoint designated individuals to develop, maintain and communicate the organization's privacy and security programs.

6 You are responsible for the actions of your third parties. Ensure that vendor contracts contain provisions that align with the organization's privacy practices and expectations.

7 Conduct an assessment of the privacy practices of the business to ensure they agree with the requirements of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Develop an action plan to address any gaps. The Office of the Privacy Commissioner of Canada has created an e-learning tool for retailers to assist in completing the assessment: **www.privcom.gc.ca/privacy_comm/0001_home_e.asp**

GENERAL DATA PROTECTION TIPS

1. Do not collect more data than required to fulfill the specific purpose. Practice data minimization and make data anonymous where detailed personal information is not required for the particular usage.
2. Review your data retention practices and securely dispose of personal information when there is no continued valid use.
3. If you require customers to show photo identification, do not record the personal information from the identification and only compare the information with the credit card.
4. Truncate credit card numbers on receipts.
5. Store customer and employee information securely in locked safes within restricted areas.

DATA PROTECTION TIPS FOR PAPER RECORDS

1. Purchase a paper shredder and shred all personal and confidential information. For large volumes of paper, engage the services of an external paper shredding company to manage your secure disposal needs.

DATA PROTECTION TIPS FOR ELECTRONIC RECORDS

1. Hire an external company specializing in the disposal of electronic storage devices to ensure that data is securely erased and completely unrecoverable.
2. Deploy information security appropriate to the size and nature of your business. Use data encryption technology appropriate to the sensitivity of the data. Engage the advice of information security consultants.
3. Secure your computer hardware to prevent the physical theft of data. Lock computers in place with secure cables and restrict access to areas of the business containing computer hardware.
4. Whenever possible, encrypt electronic data.
5. Use passwords for all computers and ensure they are confidential, complex and changed on a regular basis.
6. Back up all data necessary to ensure continuous operations of your business, and use secure storage methods to safeguard your backups.
7. Refer to the Electronic Crime section for more information on this topic.

EXTERNAL WEB RESOURCES

Office of the Privacy Commissioner of Canada
www.privcom.gc.ca/index_e.asp

Information and Privacy Commissioner of Ontario
www.ipc.on.ca/

Information and Privacy Commissioner of British Columbia
www.oipcbc.org/

Information and Privacy Commissioner of Alberta
www.oipc.ab.ca/

Information and Privacy Commissioner of Manitoba
www.ombudsman.mb.ca/

Information and Privacy Commissioner of New Brunswick
www.gnb.ca/0073/index-e.asp/

Information and Privacy Commissioner of Newfoundland and Labrador
www.gov.nl.ca/oipc

Information and Privacy Commissioner of Nova Scotia
www.gov.ns.ca/foiro

Information and Privacy Commissioner of Prince Edward Island
www.assembly.pe.ca/index.php3?number=1013943

Information and Privacy Commissioner of Saskatchewan
www.oipc.sk.ca

Commission d'accès à l'information du Québec
www.cai.gouv.qc.ca/index-en.html

SECURITY OF BUSINESS PREMISES

Addressing security issues quickly and employing some basic risk management principles can reduce the risk of crime for business, staff and customers. This section provides important security advice and information; however, it is not intended to replace privately contracted security advice.

The main aim of business security is to:

- prevent offenders from targeting the business
- reduce the impact that crime can have on a business
- reduce the rewards for the offender
- increase the effort required to access the premises and steal goods
- increase the likelihood of an offender being identified and caught
- assist police in apprehending offenders

Your level of security should depend on:

- the type of business you operate
- the nature of the business or stock
- the period of time that the premises are unoccupied
- the location of the premises
- the history of offences on the premises or inside the business

PREVENTION

BASIC SECURITY TIPS

1. Make sure laneways and other external areas are well lit. Lighting should be in good working order and regularly inspected.
2. Prune all trees and shrubs around your building to enable clear visibility. Ensure that this is maintained.
3. Clear all building perimeters, including fences, of refuse and potential climbing aids.
4. Maintain well-built and adequately secured boundary gates and fences.
5. Fully secure all external doors and windows with locking devices of good quality. Make sure they are regularly maintained. All doors should be of solid construction and well fitted.
6. Fasten steel doorjamb strengtheners to door frames.
7. If padlocks are required to secure fixtures or items, confirm that selected locks meet or exceed industry standards.
8. Consider installation of security bars, screens, grills, or roller shutters on vulnerable windows and/or skylights.
9. Consider installation of bollards, heavy planters or large rocks to act as barriers.
10. Consider installation of a monitored security alarm system.
11. Prominently display signs that indicate the presence of a security system, the continual surveillance of the premises and any other security measures present.
12. Consider installing electronic sensors to advise staff when customers enter and leave the business.
13. Install a quality surveillance camera that will act as a deterrent and help police identify offenders.
14. Minimize posters and curtains on store windows (where possible) to maintain visibility to and from the street.
15. Ideally, standalone shelves should be no more than 1.6 metres high, thereby enabling clear visibility throughout the store by staff.
16. Secure and register all property of value, including details of make, model, serial number, and description.
17. Clearly and permanently mark all property with your store name or other identifying information.
18. Never leave large amounts of cash on premises overnight. Banking should be conducted during working hours.
19. If a safe is present on site, ensure that it is located in a secure position and affixed to a solid object.
20. Ensure all staff understand and obey lock-up procedures.
21. Advise local police and any security provider of emergency after-hours contacts for the business.

RCC the voice of retail
Retail Council of Canada
www.retailcouncil.org

RBC
www.rbc.com

CLOSED CIRCUIT TELEVISION (CCTV)

Locate CCTV cameras in:

- after-hours areas that have little or no natural surveillance from passing motorists, pedestrians or employees.
- areas at risk to vandalism, graffiti or other criminal offences.
- high-risk areas, such as computer rooms or cash-handling areas, that are not adequately protected by staff surveillance.
- entrances, exits, front counter areas and other high-traffic areas.

Equipment considerations

- Use cameras with digital lenses that provide high-quality images.
- Connect video recorders to computer hard drives that can record continually. The actual digital video recording system, as opposed to the monitors, should be stored in a locked room, not viewable or accessible from the main store.
- Install copying facilities so that you can give police a copy of recorded footage.
- Clearly display signs reminding customers that all activity is recorded. Place monitors in a prominent position easily observable by staff.
- Replace tapes regularly to protect image quality.

It is important that staff know how to operate security equipment and that you test and check equipment regularly.

Position of cameras

- Install cameras at places where offenders are most likely to have to pass or want to access, such as building entry and exit points, cash registers, rear storerooms and areas where high-value items are kept.
- Cameras should be placed to record faces, not peoples' backs.
- Make cameras clearly visible to deter potential offenders.
- Place cameras at a height that captures a full view of the offender's face without being obscured by other interferences.
- Ensure surveillance areas have sufficient lighting.

Police require the largest possible facial image of an offender. The usefulness of facial images largely depends on the quality of the cameras and placement of cameras. Do not position cameras at heights that only provide vision of the top of a person's head.

KEY/ACCESS CARD CONTROL

- Maintain strict control of keys and cards.
- Utilize security keys/cards that cannot be copied without authorization.
- Maintain a formal key/card register and monitor their issue and return.
- Utilize a lockable key/card storage cabinet for keys that controls access.
- When not in use, keys/cards should be kept in a lockable steel cabinet located in a secure area. Maintain strict control of all keys/cards.
- Keys/cards should be restricted to a minimum number of people and retrieved from ex-employees.

PRIVATE SECURITY

When selecting a security firm, ensure that the firm is registered with the provincial government, bonded, and comes with a reputation for quality service. To check whether a company is reputable, ask for professional accreditations and associations.

ADDITIONAL INFORMATION

Many local law enforcement agencies in Canada provide additional security tips and best practices. These are often delivered by their crime prevention and business watch community program.

NOTES

RETAIL BUSINESS SECURITY SELF ASSESSMENT

Retail Council of Canada (RCC) and Royal Bank of Canada (RBC) are pleased to provide you with this Retail Business Self Assessment which has been designed to help business owners, operators and staff to assess the security of their business. The self assessment covers potential areas of vulnerability, and provides suggestions for adapting your security to reduce the risk of crime against your business.

Complete each question in the Retail Business Security Self assessment. If you answer "No" to any of the questions, review the suggested treatment options attached.

RCC is committed to ensuring the saftey of retailers, their staff and property. It is intended that use of the recommendations contained in this package may minimize the likelihood of criminal activity in and around your place of business. Use of the recommendations however does not guarantee that all risks have been identified, or that the area evaluated will be free from criminal activity if the recommendations are followed. Use of these recommendations is not intended to replace expert and specialized legal or security advice that may be relevant to your business.

Please visit RCC's website at www.retailcouncil.org for further information.

NO.	QUESTION	YES	NO	N/A	COMMENTS
BUSINESS IDENTIFICATION					
1	Is the business address clearly visible from the street?				
2	Is the business name clearly displayed?				
3	Is the business identifiable from the rear of the building?				
WARNING SIGNS					
4	Are there appropriate warning signs posted around the perimeter of the property?				
5	Are there appropriate store signs to guide visitors?				
6	Are the signs clearly visible?				
LANDSCAPING					
7	Is landscaping around the business free from potential hiding places?				
8	Is landscaping regularly maintained?				
9	Is the business free from landscaping that would provide offenders access to areas of the business?				
FENCES & GATES					
10	Are there fences erected around the business?				
11	Are gates locked after business hours?				
12	Are fences and gates around the property able to restrict access after business hours?				
13	Are the fences in good condition?				
14	Are the gates in good condition?				
SECURITY LIGHTING					
15	Is there security lighting installed around the business?				
16	Is the security lighting operating?				
17	Is the business well lit?				
18	Are entry and exits well lit?				
19	Do you leave limited lighting inside the business on all night?				
20	Is lighting positioned in a way to reduce opportunities for vandalism?				

NO.	QUESTION	YES	NO	N/A	COMMENTS
BUILDING DESIGN					
21	Is the building of solid enough construction to restrict unauthorized access?				
22	Is there adequate protection against entry via the roof?				
23	Is the height of the counter appropriate for the business?				
24	Can the counter be seen from outside the business?				
25	Are customers prevented from accessing the area behind the counter?				
26	Are customers prevented from accessing the back room?				
27	Is shelving arranged to provide good sightlines within the store?				
MAILBOX					
28	Is your mail inserted into your door?				
29	Is your mailbox fitted with an appropriate lock?				
DOORS					
30	Are the business' external doors of solid construction?				
31	Are these doors fitted with quality lock sets to restrict access?				
32	Are entry / exit points clearly identified?				
33	Are all fire exit doors self-closing?				
34	Are exit doors used appropriately by staff?				
35	Are at-risk doors locked at all times?				
36	Are external door hinges mounted so they cannot be removed?				
WINDOWS					
37	Are external windows to the business of good construction?				
38	Are these windows fitted with quality locks?				
39	Are windows free of promotional materials?				
40	Are skylights secured?				

NO.	QUESTION	YES	NO	N/A	COMMENTS
PROPERTY IDENTIFICATION					
41	Have you recorded make, model and serial numbers of your business items (such as cell phones, computers, etc.)?				
42	Is all valuable property permanently marked with a corporate identifier?				
43	Is your property photographed for identification?				
44	Do you have the appropriate level of insurance?				
45	Are your property list and photographs kept somewhere safe?				
TELEPHONES					
46	Are your telephones pre-programmed with emergency contact numbers?				
47	Can the telephone line be accessed in an emergency?				
SAFES					
48	Do you have a safe installed?				
49	Is the safe securely anchored?				
50	Does the safe have a drop-chute facility?				
51	Is the safe kept locked?				
52	Do your employees have the safe's combination?				
KEY AND VALUABLES CONTROL					
53	Do you have a key register?				
54	Are all spare keys secured / numbered?				
55	Are keys to the safe adequately secured?				
56	Does staff have a location to secure their personal items?				
57	Does this location have restricted access?				
CASH HANDLING					
58	Do you have established cash-handling procedures?				
59	Do you have a lockable cash drawer?				
60	Do you have irregular banking procedures?				
61	Is a company used to transport cash?				
62	Is money counted out of public view?				
63	Do you reconcile daily?				

NO.	QUESTION	YES	NO	N/A	COMMENTS
INTRUDER ALARM SYSTEMS					
64	Is an intruder alarm system installed?				
65	Is the intruder alarm monitored?				
66	Does the system work?				
67	Do you check the system on a regular basis?				
68	Does the alarm system need upgrading?				
69	Do each of your employees have their own password for the alarm system?				
SURVEILLANCE EQUIPMENT					
70	Do you have surveillance equipment installed?				
71	Is footage recorded on video / DVR?				
72	Are cameras monitored?				
73	Does the business have a customer TV monitor?				
74	Is the business free of dummy cameras?				
75	Does the camera system need upgrading?				
76	Are cameras suitably positioned?				
77	Are videos downloaded regularly?				
78	Is video footage kept for a minimum of one month?				
OCCUPATIONAL HEALTH & SAFETY					
79	Is management aware of their obligations under the Provincial Occupational Health & Safety laws?				
80	Are staff aware of their obligations and rights under the Provincial Occupational Health & Safety laws?				
81	Have staff been provided with information and training about Occupational Health & Safety?				
GENERAL					
82	Do you have security services onsite?				
83	Do security services patrol your site?				
84	Are sensitive documents appropriately destroyed?				
85	Are computer passwords changed regularly?				
86	Do you have an emergency evacuation plan?				
87	Does staff understand the plan?				
88	Are garbage bins suitably located?				
89	Do you keep sensitive documents onsite?				

NOTES

SUGGESTED BUSINESS SECURITY MEASURES

If you answered no to any of the questions in the Retail Business Security Self-Assessment, you may want to consider making some changes. The changes below will help reduce the risk to you, your business and your staff. If you need more advice or assistance, please contact your local police department or RCMP detachment.

BUSINESS IDENTIFICATION

- The street/store number must be prominently displayed at the front of your business.
- The number should be a minimum height of 120 mm and be visible at night.
- The number could also be painted on the street curb outside your business to help emergency services and visitors locate your business.

WARNING SIGNS

- Effective signage and/or directional signs should be considered to provide additional guidance to visitors in locating reception areas.
- It can also assist in controlling activities and movements throughout the premises and grounds.
- Post warning signs around the perimeter of the business to warn intruders of what security measures have been implemented to reduce opportunities for crime.

  Examples: *Warning - Trespassers will be prosecuted.*
  Warning - This property is under electronic surveillance.
  Warning - No large amounts of cash are kept on these premises.
  All property has been marked for police identification.

LANDSCAPING

- Keeping trees and shrubs trimmed can reduce concealment opportunities and increase visibility when traveling to and from the business.
- Remove obstacles and trash from property boundaries, footpaths, driveways, car parks and buildings to reduce concealment opportunities and prevent offenders from scaling your building.

FENCES AND GATES

- Install quality security fences around the perimeter of your business to clearly define the property boundaries and restrict access, preferably open-style fencing and gates of similar construction to prevent an offender from using the fence for concealment.
- All gates should be kept shut and locked when not in use.
- Fences and gates should be maintained to assist with the protection of your property.

SECURITY LIGHTING

- Install security lighting in and around your business, particularly over entry/exit points to create an even distribution of light with no glare; e.g., sensor lighting or floodlighting.
- Leave a limited amount of internal lighting on at night to enable patrolling police, security guards or passersby to monitor activities within the business.

RCC the voice of retail
Retail Council of Canada
www.retailcouncil.org

RBC
www.rbc.com

BUILDING DESIGN

- The floors, walls and ceilings should be of solid construction.
- The roof should be reinforced with mesh below the roofing to restrict unauthorized entry.
- Maintain clear sightlines between the street, neighbouring property and the buildings.
- Posts or barriers can be installed to reduce the opportunity for smash-and-grab attacks.
- Limit the number of entry/exit points to restrict unauthorized access.
- Counters should be designed to reduce the opportunity for assault of staff and unauthorized access.
- Consideration should be given to the width, height and location of the counter.
- Shelving should be limited in height or constructed of transparent materials to increase natural visibility of the premises.
- Shelves should be positioned to maximize supervision from counter area.
- The power board should be housed within a metal box and secured with an approved lock to restrict unauthorized tampering with the power supply.

MAIL RECEPTACLES

- Mail receptacles should be secured with quality locks to restrict unlawful access to your mail.

DOORS

- External doors and frames should be of solid construction and comply with the municipal building code.
- The doors should be fitted with single-cylinder lock sets which comply with the municipal building code. A single-cylinder lock set is key-operated on the external side with either a turn latch or handle on the inside to enable occupants to escape in an emergency, such as fire or other life-threatening situation.

WINDOWS

- Windows and frames should be of solid construction.
- Windows should be fitted with key-operated window lock sets to restrict unauthorized access.
- Glass may also be reinforced with a shatter-resistant film to restrict unauthorized access. Other options include replacing the existing glass with laminated glass or having quality metal security grilles or shutters installed.
- No more than 15% of display windows should be covered with promotional materials to increase surveillance opportunities to and from the business.

PROPERTY IDENTIFICATION

- Record descriptions/model/serial numbers of property for easy identification.
- Back up property lists and store separately from your hard drive in case the computer is lost or stolen.
- Engrave or etch your property with a traceable number for identification. When you sell your property, place a neat line through your engraving to show that it is no longer valid.
- Always provide a receipt of sale.
- Photograph and record the details of unique items to aid in their recovery if stolen.
- Ensure that you have adequate insurance for the replacement of property.
- Your property list, photographs and other documentation should be adequately secured in a safe or safety deposit box.
- For items that cannot be engraved, you can mark them with an ultraviolet pen, which produces markings visible only under an ultraviolet (black) light.

RCC the voice of retail
Retail Council of Canada
www.retailcouncil.org

RBC
www.rbc.com

TELEPHONES

- Telephones should be pre-programmed with the emergency number 911 and your local police number for quick reference.
- Telephone lines or boxes should be secured to avoid unlawful tampering.

SAFES

- A safe designed and installed to Insurance Bureau of Canada and/or RCMP standards should be utilized to provide additional security to money and other valuables.
- The safe should be anchored to the floor to prevent easy removal.
- The safe should have a drop-chute facility installed to enable staff to deposit money without having to open it.
- The safe should be locked at all times when not in use.
- Further consideration should also be given to using a time-delay facility to restrict access to the safe.
- The safe should be installed in an area away from public view where access is limited.
- Only management personnel should have access to the safe.

KEY AND VALUABLES CONTROL

- The control of keys and valuables is very important and should be closely monitored by management.
- A key register should be used to list which staff members have been issued with keys, the type of keys issued and what areas they can access.
- A register should also be used to record which staff members have been issued with valuable items such as laptop computers, mobile phones, etc. These registers should be detailed and regularly maintained and audited.
- Where possible, all valuables should be clearly marked with the business's details. Serial numbers and other details should be recorded and stored in a safe place.
- To reduce the likelihood of theft and or damage, try to limit the number of keys and valuables left unsecured and in plain sight of potential intruders.

CASH-HANDLING PROCEDURES

- Establish clear cash-handling procedures within your business to reduce opportunities for crime.
- Try to reduce the amount of cash your business deals with.
- Limit the amount of money carried in the cash drawer at any time.
- Lock cash drawers when not in use and clear money from the cash drawer on a regular basis.
- Avoid counting cash in view of the public.
- Use a minimum of two staff or security services when transferring money to financial institutions, or consider using a reputable security company, especially when transferring large amounts of money.
- Where possible, limit cash amounts by installing electronic payment systems.
- Don't use conspicuous bank bags when transferring money.
- Avoid wearing uniforms or store identification when transferring money.
- Establish a robbery prevention program.
- Cash transactions should be reconciled daily in order to detect/report financial irregularities.

INTRUDER ALARM SYSTEM

- Install a monitored intruder alarm system that has been designed and installed to the National Fire Code of Canada and Underwriters Lab of Canada standards to enhance the physical security of your business.
- As a number of premises have had telephone lines cut to prevent alarms being reported to the security monitoring company, a supplementary system such as Global Satellite Mobile (GSM) or Radio Frequency (RF) systems should be used to transmit the alarm signal by either mobile telephone or radio frequency.
- Consideration should also be given to incorporating duress devices into the system to enable staff to activate the system manually in the event of an emergency, such as a robbery. ***Duress devices should only be used when it is safe to do so.***
- LEDs (red lights) within the detectors should be deactivated, to avoid offenders being able to test the range of the system.
- The system should be tested on a regular basis to ensure that it is operating effectively.
- If you have a system installed within your business, use it.
- Staff should be trained in the correct use of the system.
- All staff members should have their own PIN number.

SURVEILLANCE EQUIPMENT

- Cameras should be installed in and around the business to maximize surveillance opportunities.
- Digital or video technology should be used to record images from the cameras.
- Recording equipment should be installed away from the counter area to avoid tampering.
- Videotapes need to be replaced often to maintain quality images.
- Installed surveillance equipment should be maintained in working order and regularly tested.
- If the surveillance system is installed, use it.
- Staff should be trained in the correct use of the system.
- Any surveillance system should be manufactured and installed by a qualified and reputable company and regularly function tested.
- Ensure that your security measures adhere to all applicable privacy laws.

GENERAL SUGGESTIONS

- Some businesses or locations may require onsite security to enhance physical security.
- Security services may be used to randomly patrol your business, particularly in an isolated location.
- Sensitive materials, including confidential records, should be appropriately destroyed or secured.
- Computer passwords should be changed regularly to restrict access and avoid misuse by past and present staff.
- Emergency evacuation plans should be implemented and maintained by your business to assist staff and emergency services in the event of an emergency. This plan should be prominently displayed for staff to review.
- Staff should be suitably trained in evacuation procedures.

NOTES

Special Thanks to the Retail Council of Canada Loss Prevention Committee

Another Great Member Benefit from

Retail Council of Canada
www.retailcouncil.org

www.rbc.com