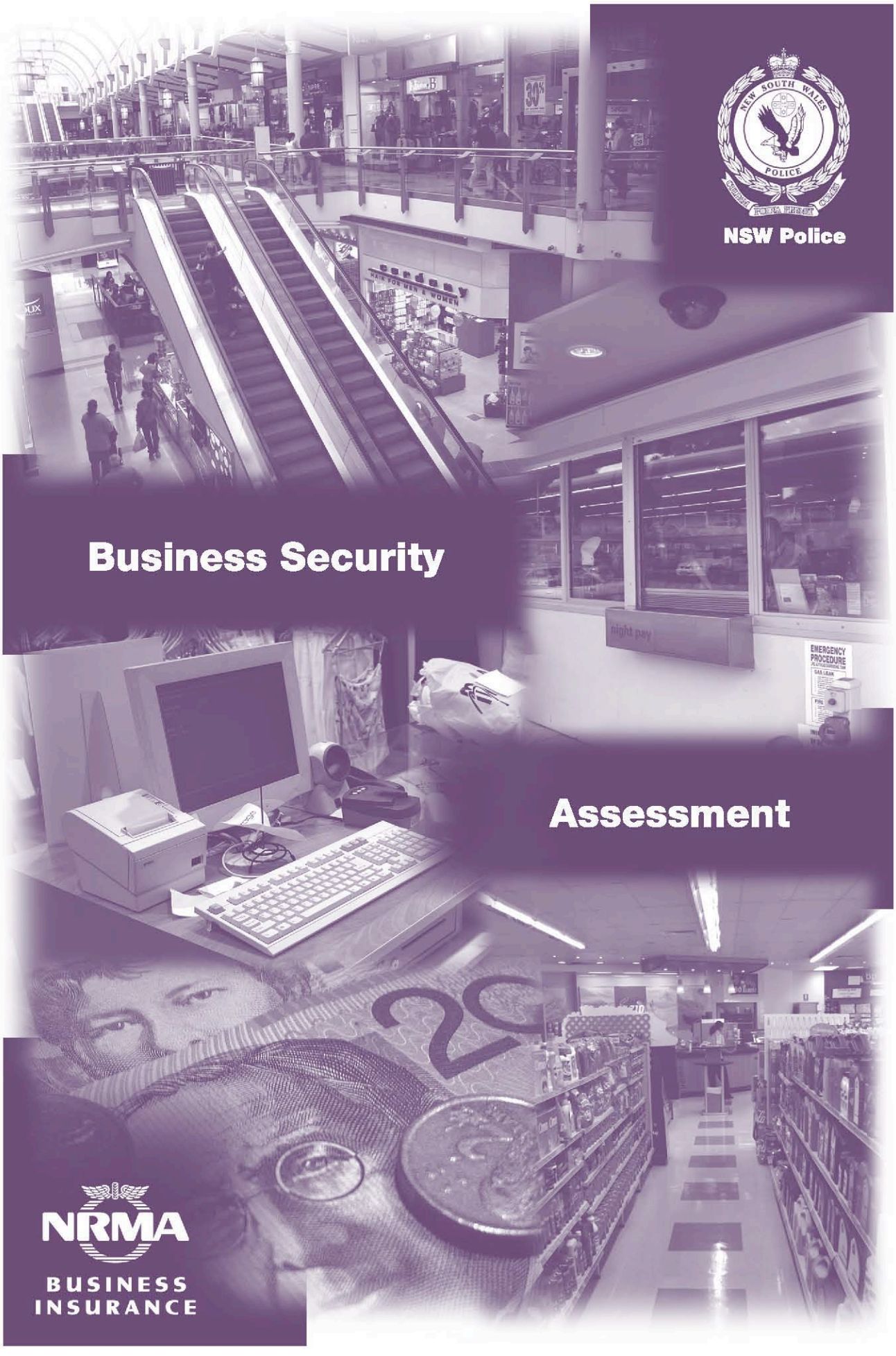
NSW Police
Business Security
Assessment
NRMA
BUSINESS
INSURANCE

Title
NSW Police Business Security Assessment

Subject
Assessment of business security

Command responsible
Operations Support Command

Available to
Unrestricted

Publication date
April 2006

Version
Two

Review date
April 2007

Publication number
0000104

NRMA BUSINESS INSURANCE

BizSafe Putting Crime Out of Business

Welcome to the NSW Police Business Security Assessment

This Business Security Assessment is designed to help business owners, operators and staff to assess the security of their business. It covers potential areas of vulnerability, and provides suggestions for adapting your security to reduce the risk of crime against your business.

You can complete the Business Security Assessment yourself, or you can ask your local NSW Police Crime Prevention Officer to undertake a Business Security Assessment of your business.

Complete each question in the Business Security Assessment. If you answer 'No' to any of the questions, review the suggested treatment options in the back of the booklet.

When you have completed the assessment, we suggest you photocopy the booklet and send a copy of the Assessment to the Crime Prevention Officer at your Local Area Command. The Crime Prevention Officer will then contact you to discuss the outcomes of the Assessment and answer any questions you may have about improving security in your business.

NSW Police has a vital interest in ensuring the safety of members of the community and their property. By using recommendations contained within this document, any person who does so acknowledges that:

- It is not possible to make areas evaluated by NSW Police absolutely safe for the community and their property
- Recommendations are based upon information provided to, and observations made by NSW Police at the time the document was prepared
- The evaluation/report is a confidential document and is for use by the person/organisation referred to on page four of this document
- The contents of this evaluation/report are not to be copied or circulated otherwise than for the purposes of the person/organisation referred to at the start of the Assessment.

NSW Police hopes that by using the recommendations contained within the document, criminal activity will be reduced and the safety of members of the community and their property will be increased. However, it does not guarantee that all risks have been identified, or that the area evaluated will be free from criminal activity if its recommendations are followed.

NSW Police Business Security Assessment

Date		Time	
Name		Business Name	
Address (Street)			
Suburb/Town		Postcode	
Telephone No		Facsimile	

Below is a checklist to help you to identify the areas where you may be vulnerable. It is not designed to cover all aspects of security, but it will identify some common vulnerabilities. Answer all of the questions.

The colour-coded boxes will help you to identify your business strengths and weaknesses.

No.	Question	Yes	No	Don't Know	Comment
Building Identification & Visitor Access (see treatment options page 10)					
1	Is the street number clearly visible from the street?	○	○	○	
2	Is the business name clearly displayed?	○	○	○	
3	Are access points supervised?	○	○	○	
4	Are visitors allowed entry to your building by appointment only?	○	○	○	
5	Do they have to report to a reception area before entry?	○	○	○	
6	Are visitors asked for proof of identification?	○	○	○	
7	Are all visitors asked to sign in when they enter the building?	○	○	○	
8	Are they provided with visitor's passes?	○	○	○	
9	Are visitor's passes designed to look different from staff passes?	○	○	○	
10	Are visitors searched before entry?	○	○	○	
11	Are visitors allowed to take bags into the target category?	○	○	○	
12	Is a cloaking/bag holding service provided at points of entry?	○	○	○	
13	Does a member of staff accompany visitors at all times while in the building?	○	○	○	
14	Are there appropriate internal signs to guide visitors?	○	○	○	
15	Are the visitor's passes cross-checked against those issued?	○	○	○	

No.	Question	Yes	No	Don't Know	Comment
16	Are all visitor's passes collected from visitors when they leave the building?	○	○	○	
17	Does staff wear identification badges at all times when in the building?	○	○	○	

Fences and gates (see treatment options page 11)

18	Does the facility have a 2.4m, or higher, perimeter fence?	○	○	○	
19	Does fencing clearly delineate the facility boundary?	○	○	○	
20	Do all gates in the perimeter fence have access control measures in place?	○	○	○	
21	Are the access control measures on vehicle gates sufficient to prevent forced vehicle entry? (e.g. ram raids)	○	○	○	
22	Are there appropriate warning signs displayed around the perimeter of the property?	○	○	○	
23	Are the fixings for the building coverings secured so that they cannot be released or removed from the outside?	○	○	○	

Access Control (see treatment options page 11)

24	Are the building external doors of solid construction?	○	○	○	
25	Are these doors fitted with quality locksets to restrict access?	○	○	○	
26	Are there good quality locks on each accessible door above ground level?	○	○	○	
27	Can internal doors be locked when left unattended for long periods of time?	○	○	○	
28	Are all fire doors self closing and fitted with noisemakers?	○	○	○	
29	Are external windows to the building of good construction?	○	○	○	
30	Are these windows fitted with quality locksets to restrict access?	○	○	○	
31	Are windows free of promotional materials?	○	○	○	
32	Do you nominate members of staff to check that all doors and windows are closed and locked at the end of the business day?	○	○	○	
33	Is landscaping well maintained to encourage good visibility around the perimeter of your building? e.g cutting back overgrown planting	○	○	○	
34	Is there security lighting installed around your building during the hours of darkness?	○	○	○	
35	Is the building well lit at night?	○	○	○	

No.	Question	Yes	No	Don't Know	Comment
36	Are there appropriate internal signs to guide visitors?	○	○	○	
37	Is the height of the counter appropriate for the business?	○	○	○	
38	Are visitors prevented from accessing the area behind the counter?	○	○	○	
39	Is shelving arranged to provide good sightlines within the building?	○	○	○	

Vehicles and Vehicle Access Control (see treatment options page 12)

40	Are all vehicles stopped before entering the building/property?	○	○	○	
41	Are bomb searches conducted on all vehicles entering the facility?	○	○	○	
42	Do the searches include underneath, cabin and cargo spaces?	○	○	○	
43	How close can vehicles be parked to the building?	○	○	○	
44	Will site security inspections identify an unattended vehicle immediately?	○	○	○	
45	Are unattended vehicles investigated immediately they are discovered?	○	○	○	
46	Are there specific procedures for dealing with unattended vehicles found to be suspicious?	○	○	○	

Property identification (see treatment options page 12)

47	Have you recorded make, model and serial numbers of your business items (such as mobile phones, computers etc)?	○	○	○	
48	Is all valuable property permanently marked with a corporate identifier (such as ABN)?	○	○	○	
49	Is your property photographed for identification?	○	○	○	
50	Do you have insurance?	○	○	○	
51	Are your property list and photographs kept somewhere safe?	○	○	○	

Telephones (see treatment options page 12)

52	Are your telephones pre-programmed with emergency contact numbers?	○	○	○	
53	Can the telephone line be unlawfully tampered with?	○	○	○	

Safes (see treatment options page 12)

54	Do you have a safe installed?	○	○	○	
55	Is the safe securely anchored?	○	○	○	

No.	Question	Yes	No	Don't Know	Comment
56	Is the safe in an appropriate position?	○	○	○	
57	Does the safe have a drop-chute facility?	○	○	○	
58	Is the safe kept locked?	○	○	○	

Key and valuables control (see treatment options page 13)

59	Do you maintain a key register?	○	○	○	
60	Are all spare keys secured?	○	○	○	
61	Are keys to the safe adequately secured?	○	○	○	
62	Have you supplied police with a current emergency contact list?	○	○	○	
63	Do staff have a location to secure their personal items?	○	○	○	
64	Does this location have restricted access?	○	○	○	

Cash handling (see treatment options page 13)

65	Do you have established cash-handling procedures?	○	○	○	
66	Do you have a lockable cash drawer?	○	○	○	
67	Do you have irregular banking procedures?	○	○	○	
68	Is a company used to transport cash?	○	○	○	
69	Is money counted out of public view?	○	○	○	

Personnel security (see treatment options page 13)

70	Is there a security guarding service on site?	○	○	○	
71	Have security personnel received formal security training?	○	○	○	
72	Do security personnel hold current state security licences?	○	○	○	
73	Are specific security checkpoints and other duties assigned appropriately?	○	○	○	
74	Are specific security incident response immediate actions assigned for:				
	• Unattended vehicle?	○	○	○	
	• Trespasser?	○	○	○	
	• Unauthorised access?	○	○	○	
	• Suspect package?	○	○	○	

Security Alarm Systems (see treatment options page 13)

75	Is the building protected by an onsite security alarm system?	○	○	○	
76	Is the security alarm system monitored by onsite personnel who are able to respond immediately?	○	○	○	

No.	Question	Yes	No	Don't Know	Comment
77	Does the security alarm system have a duress facility?	○	○	○	
78	Does the system work?	○	○	○	
79	If you have a burglar alarm are your staff familiar with the procedures for turning it on and off? (In order to reduce the activation of false alarms)	○	○	○	
80	Is the system checked on a regular basis?	○	○	○	

Closed Circuit Television (CCTV) (see treatment options page 14)

81	Do you have CCTV equipment installed?	○	○	○	
82	Are cameras monitored?	○	○	○	
83	Do the CCTV cameras cover the entrances and exits to your building?	○	○	○	
84	Do you have CCTV cameras covering critical areas in your business, such as server rooms or cash offices?	○	○	○	
85	Do you store the CCTV images in accordance with the evidential needs of the police?	○	○	○	
86	Could you positively identify an individual from the recorded images on your CCTV system?	○	○	○	

Information security (see treatment options page 14)

87	Do you lock away all business documents at the close of the business day?	○	○	○	
88	Do you have a clear-desk policy out of business hours?	○	○	○	
89	Do you close down all computers a the close of the business day?	○	○	○	
90	Are all your computers password protected?	○	○	○	
91	Are computer passwords changed regularly?	○	○	○	
92	Do you have computer firewall and antivirus software on your computers?	○	○	○	
93	Do you regularly update this protection?	○	○	○	
94	Do you employ the principle of least privilege?	○	○	○	
95	Do you back up business critical information regularly?	○	○	○	
96	Does the facility IT infrastructure have current virus checking packages enabled?	○	○	○	

Communication (see treatment options page 14)

97	Do you have a security policy or other documentation showing how security procedures should operate within your business?	○	○	○	

No.	Question	Yes	No	Don't Know	Comment
98	Is this documentation regularly reviewed and if necessary updated?	○	○	○	
99	Do you have a senior manager who takes responsibility for security within your business?	○	○	○	
100	Do you regularly meet with staff and discuss security issues?	○	○	○	
101	Do you encourage staff to raise their concerns about security?	○	○	○	
102	Are you a member of a local Business Watch or a similarly constituted group?	○	○	○	
103	Do you know your local community police officer or community support officer?	○	○	○	
104	Do you speak with neighbouring businesses on issues of security & crime that might affect you all?	○	○	○	
105	Do you remind your staff to be vigilant when travelling to and from work, and to report anything suspicious to the relevant authorities or police?	○	○	○	

Bomb and Explosives (see treatment options page 15)

106	Does security awareness training include the risk of bomb or explosives detonation and what is required of staff should one occur?	○	○	○	
107	Are staff aware of the impact this might have on the building?	○	○	○	
108	Is staff aware of how to deal with a bomb threat over the telephone?	○	○	○	
109	Are records and files maintained on all bomb and bomb hoax incidents?	○	○	○	
110	Does the facility have white level inspections in place for all mail and packages received through the post or by courier delivery?	○	○	○	
111	Are X-Rays imaging machines used to scan mail and parcels?	○	○	○	
112	Are known suppliers only used?	○	○	○	
113	Are all incoming stores routinely checked?	○	○	○	
114	Are X-Rays imaging machines used to scan stores?	○	○	○	
115	Are critical points patrolled and searched for suspicious items?	○	○	○	
116	Does the building have security procedures that include bomb search procedures?	○	○	○	

No.	Question	Yes	No	Don't Know	Comment
117	Do the procedures provide guidance on:				
	• the actual search technique	○	○	○	
	• what to look for	○	○	○	
	• what to do should a suspicious item be discovered	○	○	○	
	• guidelines for evacuation	○	○	○	

Fire security (see treatment options page 15)

118	Are the fire hydrants in good working order and are they clear of obstructions?	○	○	○	
119	The location of any fire extinguishers. Are they in good condition and are they accessible?	○	○	○	
120	Does security awareness training include the risk of arson and what is required of staff should a fire occur?	○	○	○	
121	Are there current arson detection and action policies and procedures in place?	○	○	○	
122	Is the building free from flammable and combustible waste and other materials that may create a fire hazard or be exploited by an arsonist?	○	○	○	
123	Is the building free from natural flammable and combustible materials that may create a fire hazard or be exploited by an arsonist?	○	○	○	
124	Does the building have an automatic fire suppression system to extinguish small fires as immediately as they start?	○	○	○	
125	Does security awareness training include the risk of firearms or weapon attack and what is required of staff should one occur?	○	○	○	

Chemical, Biological and Radiological Attack (see treatment options page 15)

126	Are all combustible storage sites secured and emptied on a regular basis?	○	○	○	
127	Is the building force ventilated at all times when occupied?	○	○	○	
128	Is the building open to the atmosphere allowing air pollutants to disperse quickly?	○	○	○	
129	Is the building subject to frequent prevailing winds making it difficult to confine the effects of any CBR materials released?	○	○	○	

No.	Question	Yes	No	Don't Know	Comment
Occupational health and safety (see treatment options page 15)					
130	Is management aware of its obligations under the NSW Occupational Health and Safety laws?	○	○	○	
131	Are staff members aware of their obligations and rights under the NSW Occupational Health and Safety laws?	○	○	○	
132	Have staff been provided with information and training about Occupational Health and Safety?	○	○	○	
133	If you have been a victim of a robbery, have you submitted the relevant paperwork to Workcover?	○	○	○	
Victim Support (see treatment options page 16)					
134	Do you have a Victim Support Policy established?	○	○	○	
135	Have victims of crime been referred to support services?	○	○	○	
Waterfront Property Security (see treatment options page 16)					
136	Are you able to restrict access from the water?	○	○	○	
137	Do you have adequate lighting of your waterfront areas?	○	○	○	
138	Is your private property clearly identified and separated from the public space?	○	○	○	
139	If you have boats on or near your property are they adequately secured?	○	○	○	
140	Does your waterfront landscaping enable you to have clear sight lines to the water?	○	○	○	
141	Can you identify your property address from the water?	○	○	○	

What do your results show?

- Having completed the checklist, you need to give further attention to the questions that you have answered **'no'** or **'don't know'** to.
- If you answered **'don't know'** to a question, find out more about that particular issue to reassure yourself that this vulnerability is being addressed or needs to be addressed. If you answered **'no'** to any question then you need to address that particular vulnerability as soon as possible.
- Where you have answered **'yes'** to a question, remember to regularly review your security needs to make sure that your security measures are fit for purpose.

Any further comments or notes

Suggested Treatments

If you answered 'No' to any of the questions in the Business Security Assessment, we suggest you consider making some changes. These changes will help reduce the risk to you, your business and your staff.

If you need advice or assistance, please contact your local NSW Police Crime Prevention Officer.

Building Identification and Visitor Access

- The street and shop number must be displayed at the front of your business.
- The street number should be a minimum of 120mm high. This will assist emergency services and visitors to locate your property. It also ensures you comply with Section 124, Order No. 8, Local Government Act, 1993.
- Visitor access should be monitored and controlled at all entries into the building.
- Passes can assist in properly differentiating between visitors and staff throughout the building. These passes should be worn and clearly identifiable at all times.
- Maintenance and repair people will carry identification. Ask to see their ID before admitting them to your business.
- If you are in any doubt, ring their company to check their authenticity.
- It may be your business' policy to conduct bag inspections/searches. However, you do not have a legal right to search a person's bag or property. The person DOES NOT commit an offence by refusing to have their bag searched. You can ask the person to leave your building and you can refuse the person future entry into the building.

  NB: Clearly display signs that explain your business' policy, e.g. "All bags must be presented for inspection before entering/leaving the business
- Effective signage and directions will provide guidance to visitors in locating reception areas and keep visitors away from restricted areas.
- Install height markers on the inside of your doors, this will help you judge the height of offenders.

Fences & Gates

- The boundary of the property should be clearly defined by boundary fences preferably an open-style construction. This allows greater visibility to and from the street, restricts unauthorised access, and clearly defines your territorial space.
- Gates should be secured with quality hardened or alloy chains and padlocks.
- All gates should be kept shut and locked when not in use.
- Fences and gates should be regularly maintained to assist with the protection of your property.
- Information regarding the different types of locks available can be obtained by contacting Australian Standards.
- Warning signs should be strategically posted around the perimeter of your property, particularly near entry/exit points.

  to warn intruders of security measures:

  Warning: these premises are under constant surveillance

  Warning: trespassers will be prosecuted

  Warning: no large amounts of money kept on premises

  Warning: monitored alarm in operation
- Signs can also assist in controlling activities and movements throughout the premises and grounds.

Access Control

- External doors and frames should be of solid construction and comply the the Building Code of Australia (Fire Regulations).
- The doors should be fitted with single cylinder lock sets which comply with Building Code of Australia (Fire Regulations).

  NB: A single cylinder lock set is key-operated on the external side with either a turn snib or handle on the inside to enable occupants to escape in an emergency
- Windows and frames should be of solid construction.
- Windows should be fitted with key-operated window lock sets to restrict unauthorised access.
- Glass can also be reinforced to restrict unauthorised access by:
  * Applying shatter-resistant film
  * Replacing the existing glass with laminated glass
  * Installing metal security grilles or shutters
- Maintain clear lines of sight between the street, neighbouring properties and buildings.
- No more than 15% of the display area of windows should be covered with promotional materials so that surveillance opportunities to and from the business are maximised
- The floors, walls and ceilings should be of solid construction.
- The roof should be reinforced with mesh below the roofing to restrict unauthorised entry.
- Limit the number of entry/exit points to restrict unauthorised access.
- Counters should be designed to reduce the opportunity for assault of staff and unauthorised access to behind-counter areas. Consider adjustments to the width, height and location of the counter.
- If using mirrors, position them so that people cannot use them to monitor activities in your business.
- Shelving within the business should be limited in height, or transparent, to increase natural visibility within the business and to the outside of the business.
- Shelves should be positioned so that staff behind the counter have good lines of sight.
- Landscaping should be maintained regularly with trees and shrubs trimmed away from doors and windows.
- Keeping trees and shrubs trimmed can reduce concealment opportunities and increase visibility when travelling to and from the business.
- Remove obstacles and rubbish from property boundaries, footpaths, driveways, car parks and buildings to restrict concealment and prevent offenders scaling your building.

- 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, floodlighting.
- Consider installing sensor lighting which is cost effective as it only activates when movement is detected within the zone.
- Leave a limited amount of internal lighting on at night to enable patrolling police, security guards or passing people to monitor activities within the business.
- The power board should be housed within a cupboard or metal cabinet and secured with an approved electricity authority lock to restrict unauthorised tampering with the power supply.

Vehicle and Vehicle Access Control

- Boom-gates and kindred access control devices can be effective as a means of regulating vehicle movement and increasing the effort required to commit crime upon your building property and car park area.
- The configuration of parking bays can impact sightlines. Grid rows increase surveillance while offset sections and herringbone patterns can reduce vision to one or two rows.
- Bollards or barriers can be installed to reduce the opportunity for ram-raid attacks.

Property identification

- Record descriptions, model information and serial numbers of all business property for easy identification.
- Back up your property lists from your computer in case the computer is lost or stolen.
- Engrave your property with a traceable number such as your ABN (Australian Business Number) for identification.
- When you sell your property, place a neat line through your engraving to show that it is no longer valid. It is also a good idea to give the person a receipt to prove the sale of the item.
- 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 e.g. in a safe or safety deposit box.
- For items that cannot be engraved, you may wish to mark them with an ultra-violet pen. This marking is only visible under an ultra-violet (black) light.

Telephones

- Telephones should be pre-programmed with the emergency number '000' and your local police number for quick reference by occupants.
- Telephone lines or boxes should be secured with an approved lock to avoid unlawful tampering.

Safes

- A safe designed and installed to the Australian Standards can provide additional security for money and other valuables.
- Anchor the safe to the floor to prevent easy removal.
- The safe should have a drop-chute facility so that staff can deposit money without having to open it.
- Consider a time delay lock, which means that the safe can only be opened at a particular time (or times) each day.
- The safe should be locked at all times when not in use to restrict access.
- The safe should be installed in an area where access is limited and away from public view.

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 those staff members who have been issued with keys, the type of keys issued and the areas each staff member has access to.
- The control of valuables is just as important and a register should also be used to record which staff members have been issued with valuable items such as laptop computers, mobile phones, etc.
- Registers should be detailed and regularly maintained and audited.
- In addition, all valuables should be clearly marked with the business details where possible and the 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 or in plain sight of potential intruders.

Cash-handling

- 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. Use as small a float as is practical for your business.
- Lock cash drawers when not in use, and clear money from the cash drawer on a regular basis e.g. to a safe.
- If possible, have a secure area for handling and counting cash. ALWAYS keep this area secure and out of sight of the general public and access ways.
- Use a minimum of two staff, or security services, when personally transferring money to or from the bank.
- Consider using a reputable security company to do your banking especially when transferring large amounts of money.
- Where possible, limit cash amounts by installing electronic payment systems such as EFTPOS.
- Don't use conspicuous bank-bags when transferring money.
- Avoid wearing uniform or identification when moving money to or from the bank.
- Establish a robbery prevention program.

Personnel Security

- Some businesses or locations may require on-site security to enhance physical security.
- Security services may be used to randomly patrol your business, particularly in an isolated location.
- It is important to prove the identity of potential new staff. You should see original documents and not photocopied and, where possible, check the information, explaining any gaps. During recruitment do you require:
  - (a) Full name?
  - (b) Current address and any previous addresses in last five years?
  - (c) Date of birth?
  - (d) National Insurance number?
  - (e) Full details of references (names, addresses and contact details)?
  - (f) Full details of previous employers, including dates of employment?
  - (g) Proof of relevant educational and professional qualifications?
  - (h) Proof of identity is vitally important and the following documents can assist you in verifying their identity.

Security alarm systems

- To enhance the security of your business, you can install a monitored intruder alarm system.
- If you have a system installed within your business, make sure you use it.

- Ensure the system has been designed and installed to the Australian Standard (Domestic and Commercial Alarm Systems)
- Thieves have been known to cut telephone lines to prevent alarms being reported to the security monitoring company. We suggest you consider a supplementary system such as Global Satellite Mobile (GSM) or Radio Frequency (RF) systems to transmit an alarm signal.
- Consider incorporating a duress facility into the system to enable staff to activate the system manually in the event of an emergency, such as a robbery.

  NB: Duress devices should only be used when it is safe to do so
- LEDs (Light Emitting Diodes) are red lights within the detectors. They should be deactivated so that offenders cannot test the range of the system.
- The system should be tested on a regular basis to ensure that it is operating effectively.
- Staff should be trained in the correct use of the system.
- Consider only using companies licensed under the NSW Security Industry Act.
- Alarm system controls should be concealed to restrict tampering.
- Remote on/off switches should be strategically located.
- Movement detection devices should be strategically located around the premises.

Closed Circuit Television (CCTV)

- CCTV can enhance the physical security of your business and assist in the identification of people involved in anti-social or criminal behaviour.
- Cameras should be installed both within and around the business to maximise surveillance opportunities.
- Digital or video technology should be used to record images from the cameras.
- Cameras should monitor the cashier's area, high cost merchandise or areas with poor natural supervision.
- TV monitors should enable staff to monitor activities on the camera.
- Recording equipment should be installed away from the counter area to avoid tampering.
- Videotapes need to be replaced quarterly to maintain quality images.
- Installed surveillance equipment should be maintained in working order and regularly tested.
- If a 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 the requirements of the Surveillance and Privacy Act are adhered to.

Information Security

- Limit access to confidential information.
- Sensitive materials, including confidential records, should be appropriately destroyed or secured, e.g. confidential records should be shredded or disposed of through security destruction services.
- Computer passwords should be changed regularly to restrict access and avoid misuse by past and present staff.
- Cancel access promptly when people transfer or leave.

Communication

- Staff training days should be held on a regular basis reinforcing safety and security procedures of your business.
- 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.

- Avoid opening and closing your business alone if you are not operating 24 hours a day.
- Have clear policies on critical issues such as shoplifters, handling aggressive customers and cash handling.
- Encourage employees to report any suspicious activity or persons in or around the area to local police.

Bomb and Explosives

- Make sure staff are familiar with emergency procedures and what they can do if they feel unsafe in the workplace
- White level inspections should be conducted on your business on a regular basis. A white level inspection is an inspection by all staff of their respective workplaces for any articles that are unusual, suspicious or unable to be accounted for.
- White level inspections should be undertaken each day upon arrival at work and/or when instructed by the owner/manager.
- Keep a copy of a Bomb Threat Checklist under all telephones.
- If possible, fill it out while you are on the phone to the caller.
- Ensure that staff understand the form's purpose and how to fill it out.
- Report threats to the police immediately.
- Suspicious items- what to look out for:
  (a) Excessive or stained wrapping
  (b) No return address
  (c) Incorrect titles
  (d) Misspelling of common words
  (e) Excessive postage
  (f) Excessive weight
  (g) Unexpected or unsolicited mail
  (h) Markings such as 'Confidential, Private'
- Do not touch, tilt or tamper with the item. Contact police immediately on '000'. Explain what it is that makes the package suspicious. Follow the instructions given to you by police.

Fire Security

- Install an Automatic Fire Detection System.
- Ensure you have a working smoke detector in your business and that it is checked regularly.
- Ensure you have a first-aid kit that is properly stocked
- Staff should be suitably trained in evacuation procedures.

Chemical, Biological and Radiological Attack

- All air conditioning vents should be secure and checked on regular basis
- Ensure all staff are trained for emergency management of Chemical, Biological and Radiological Attack
- All combustible storage sites should be secure and emptied on a regular basis.
- Dispose of all flammable waste materials as quickly as possible.
- Waste bins should not be fixed to walls, but kept in a secure compound with padlock and chain.

Occupational Health and Safety

Duties of employers

- An employer must ensure the health, safety and welfare at work of all the employees of the employer.

- That duty extends (without limitation) to the following:
  (a) ensuring that any premises controlled by the employer where the employees work (and the means of access to or exit from the premises) are safe and without risk to health
  (b) ensuring that any plant or substance provided for use by the employees at work is safe and without risks to health when properly used
  (c) ensuring that systems of work and the working environment of the employees are safe and without risks to health
  (d) providing such information, instruction, training and supervision as may be necessary to ensure the employee's health and safety at work
  (e) providing adequate facilities for the welfare of the employees at work

Others at workplace

- An employer must ensure that people (other than the employees of the employer) are not exposed to risks to their health or safety arising from the conduct of the employer's undertaking while they are at the employer's place of work.

Victim support

If you or your staff have:

- Experienced a situation where violence or the treat of violence has occurred.
- Received an injury as a result of violence.
- Suffered a loss or adverse effects as a result of experiencing violence; or
- Experienced domestic violence or sexual assault.

You can contact the Victims of Crime Bureau by telephoning Sydney 02 9374 3000 or Toll Free 1800 633 063

Victims of Crime Bureau staff can provide or put you in contact with services you may require such as:

- Counselling (telephone or fact to face).
- Information about other support services.
- Information about legal processes.
- Information about eligibility for, and applying for, victims compensation.
- Resolving complaints about government services.

The Victims of Crime Bureau's assistance line operates 24 hours a day, 7 days a week. The telephone counselling and referral service is operated by the Victims of Crime Bureau in conjunction with Sydney City Mission.

Waterfront Properties

- Consider installing security and/or sensor lighting between your property and the water.
- Keep trees & shrubs trimmed to reduce concealment opportunities and increase visibility of the waterfront from the property.
- Create a visual barrier between your property and the water to identify where your private property starts.
- Ensure a physical barrier such as a gate and padlock is erected at the beginning of your mooring, to prevent thieves gaining access to your boat, and it will also restrict those wanting to leave your home via the water.
- Consider some type of identification marker, so you can establish from the water the identity of your property. For example the name of you home may be constructed as a sign on your waterfront property entry point.

Conclusion

NSW Police hopes that by using the recommendations contained within this document, criminal activity will be reduced and the safety or members of the community and their property will be increased.

NSW Police would like to thank you for your interest in improving the security of your business and in preventing crime in our community.

Should you need any further information on the subjects covered by the Business Security Assessment, we encourage you to contact your local NSW Police Crime Prevention Officer.