Good Security

Good Business

Good Security

Good Business

Attorney-General's foreword

Small business plays a crucial role, not only in our nation's economy but in Australian society.

We often make decisions about where we reside based on the services made available by small business, whether in the city, the suburbs or rural areas. Communities rely on small business for services and employment as well as support for various sporting and social activities.

But what if for some reason these businesses were disabled for any length of time? How would this disrupt daily life and the wellbeing of the community? And what will be the key to businesses quickly returning to normal operations?

What we have come to realise is that the cause of a disruption to service is of little relevance to those who rely on it. Having no access to food or a doctor, for example, brings the same problems, stress and, potentially, trauma whether the cause is a flood, criminal activity or a pandemic.

The point of difference between a business that recovers quickly and one which struggles to bounce back under similar circumstances is organisational resilience. Those businesses that embrace resilience greatly improve their chances of not only surviving an adverse event but of potentially thriving.

With the building of organisational resilience comes flexibility and the ability to adapt to changing environments. No organisation can anticipate every challenge and although money and resources play their part, thinking about how to face the challenges of the unexpected is the basis of good resilience planning.

Business continuity and risk management help us to prevent what can be prevented and protect what can be protected. Resilience enables us to cope with what we cannot prevent or protect.

This booklet outlines how you can make your business more resilient by understanding how your business operates, identifying and evaluating risks, and developing emergency and continuity plans. In short, making security planning an integral part of your business.

Also contained in this second edition of Good Security, Good Business are details of the new National Counter-Terrorism Alert System.

The new system means alert levels can now be applied where necessary – across the nation or for specific communities, industry/business sectors, or geographic locations. This will help avoid unnecessary disruptions to everyday life – a more logical approach that I believe will be welcomed by the public and private sector alike.

I encourage all small and medium business owners to read this booklet as a starting point for building a more resilient organisation. Your vital role in the lives of Australians is indisputable but beyond this is the reality that good security is good business.

Attorney-General,
The Hon Robert McClelland MP

Plan now and protect your business

If you run a business, you will know that success does not come easily.

Business survival and profitability requires good planning, good management, self-belief and a lot of hard work.

It also requires planning for the unexpected. In addition to the constant pressures of the marketplace, your business is at risk from a range of hazards outside your control.

Anything from a burst water pipe, a fire, an earthquake, a criminal act or even a terrorist attack could affect your business, your livelihood, your safety and the safety of those who work with you.

Planning for an incident and working out how your business will respond and recover are some of the most important things you can do.

The time for planning is now. How well you survive and move forward from an incident will depend on the measures you put in place beforehand.

Small businesses employ over three million Australians and generate around 30 per cent of economic activity.

Good security – good for business …

Planning to manage risk should be an essential part of your business planning.

If you are ready for an incident of any kind its impact will be less, your recovery will be quicker and easier, and you will be in a better position to achieve your long-term goals.

Good security planning even has business benefits – building customer confidence and enhancing your reputation.

… and good for Australia

Small businesses are the backbone of the Australian economy.

Australia needs its small businesses to be strong and resilient.

A small business sector that is ready for an incident and is able to bounce back quickly will benefit us all.

Good planning will help your business survive and recover from an unexpected incident.

What to do

Good security planning is really just common sense.

The steps involved are easy to understand and apply to your business.

- **Know your business**

  Understand how your business works and know what things are vital to its ongoing operation.

- **Identify the risks**

  Identify the risks your business might face.

- **Analyse the risks**

  – What is the likelihood of these risks occurring?
  – What would the impact be?

- **Evaluate the risks**

  Weigh up the risks and decide what needs to be done to treat them.

- **Develop an emergency plan**

  Develop a plan to guide your response to an incident.

- **Develop a continuity plan**

  Plan what will need to be done to get your business going again.

Some simple planning will protect your business.

- **Make security planning part of your everyday business**

  Good planning is good business. By regularly reviewing your plans, you will be in the best possible position to minimise risks, manage any incident and move forward afterwards.

Understanding your business is the first step in protecting it.

Know your business

Properly preparing for an incident means understanding in detail how your business operates.

What are your goals? What drives your business and makes it successful?

Take into account things like:

- Are there certain systems or suppliers that you could not do without?
- What technical systems do you need to keep going?
- Are there records or information your business could not survive without?
- Are there computer passwords, office keys or safe combinations that are essential?
- Are there people outside your business you depend on or who depend on you?
- Are there legal or contractual obligations you need to meet as part of your daily business?

Identify the risks …

Knowing what risks your business faces will help you decide what planning needs to be done.

Think about the sorts of things that could affect your business.

- Natural disasters – fire, flood, cyclone.
- Human threats – crime, computer hackers, terrorism.
- Influenza pandemic – resulting in widespread social and economic disruption and employee absenteeism.
- Other unforeseen events – power failures, gas leaks, burst water pipes, supplier problems.

Ask yourself when, where and why these things could happen and what the impact would be.

What if:

- The power failed?
- Your computers and business records were destroyed?
- The telephone system or Internet went down?
- You or your workers were seriously injured or unable to come to work for a prolonged period because of an infectious disease or pandemic?
- The roads were blocked, public transport systems were not working or there was limited access to fuel?
- You had to leave your premises or had to find new ones?
- Your insurance was inadequate?

Managing risks requires an understanding of threats, the dangers they pose and the likelihood that they could occur.

Also think about what would happen if your relationship with customers and suppliers changes.

What if:

- You could not easily contact your customers or they could not contact you?
- Your suppliers went out of business?

… and analyse the risks

How likely is it that any of the identified risks will occur?

It is good sense to plan for things that may happen – but it may be a waste of time and resources to plan for things that are highly unlikely to occur.

By knowing the risks, understanding the possible consequences and estimating the chances of an incident happening, you will be in a good position to prepare, survive and move forward from an incident.

Work out your approach to risk – different circumstances require different approaches.

Evaluate the risks

The next task is to decide what your approach to risk is and what needs to be done.

- Are you prepared to accept some risks?

  – This may mean not doing much planning at all.

- Are you 'risk averse' and keen to minimise risk as much as possible?
  – This may mean putting in place detailed plans and spending the required time, effort and resources.

- Or are you somewhere in between?

Sometimes, risks may be so unlikely, or the solutions so complex and costly, that you may decide that it is not worthwhile or practical to address them.

Every business will have a different approach to risk. Think about the risks you face and the value you place on being able to manage an incident and recover quickly.

A straightforward emergency plan will outline what needs to be done for your business to successfully manage an emergency incident.

Develop an emergency plan

You are now ready to develop an emergency plan.

It is essential that your plan is straightforward and is embraced by you and your employees.

The plan will work best if everyone understands their responsibilities and what they will need to do in the event of an emergency.

The types of things that should be covered in an emergency plan include:

An evacuation strategy

- Monitor the media and take advice from authorities.
- Identify evacuation routes and emergency assembly sites to account for workers.
- Identify who has the authority to order an evacuation.
- Establish a chain of command to ensure that all key roles and responsibilities are covered.

Emergency supplies

- Have a first-aid kit and advise employees of its location.
- Identify people who have completed first-aid training and train staff if necessary.

Coordinate your plan with others

- Fire is the most common threat to businesses – know what to do if a fire starts.
- Talk to emergency service providers such as police, fire and ambulance services and know what they will want you to do if an incident happens.
- Meet with your neighbours and other businesses to compare plans and avoid confusion.
- Inform your customers and suppliers about your plan – this will let them know you are serious about surviving an emergency.
- For major incidents, such as a flu pandemic, the government will activate special plans. *The Australian Health Management Plan for Pandemic Influenza* is available at www.health.gov.au.
- *The National Action Plan for Human Influenza Pandemic* sets out responsibilities, lines of authority and cooperative arrangements between Commonwealth, State, Territory and local governments.

  The National Action Plan for Human Influenza Pandemic is available at pmc.gov.au/publications/pandemic/.
  The Australian Government has also produced a business continuity guide to assist planning and preparedness by business in the event of an influenza pandemic. The guide is available at www.industry.gov.au/pandemicbusinesscontinuity.

Understand your business, the risks it faces and the things that need to be done to manage an incident and move forward.

Secure your business

- Determine which machinery, equipment, cabinets or safes may need to be secured.
- Identify people to lock doors and secure your premises.
- Ensure that responsible staff have the right keys, passwords or combinations.
- Decide whether a special security plan is needed for your computer systems.

Consider developing a specific security plan

- How would you protect your information, your premises and your staff?
- Work out how you would deal with a threat to your business, such as a bomb threat.
- Regularly practise and refine your security plan.

Insurance

- Speak with your insurance company and make sure you are properly insured.

Communication plan

- Work out how you will communicate with emergency services, your employees, customers and suppliers in the event of an incident.

Make checklists

- Checklists can help to ensure that your plan gets put into practice.
- Set out what needs to be done, by whom and when. Identify backups for key jobs in case someone is away.
- It can be a good idea to set out what needs to be done immediately and what needs to be done in the following 24 or 48 hours.

Develop a continuity plan

Once the immediate threat has passed, your profitability and the survival of your business depends on getting things back to normal as soon as possible.

Your business continuity plan follows on from your emergency plan. Its purpose is to identify what needs to be done to bounce back quickly.

In the case of an influenza pandemic, you may need to consider business continuity over a period of two to three months, with possible staff absences of up to 50 per cent during that period.

Identify how your business operates

What things are essential to your business functioning properly?

Ask questions like:

- Who are my key people?
- What things must be done for my business to operate?
- Are there computer systems, documents or records that I could not do without?
- Does my business rely on particular suppliers?

The businesses that bounce back after an incident are the ones that have prepared and put practical plans in place.

Work out how your business can continue

- Once you know the critical things that make your business work, you need to think about how you can get them going again or how you could go forward without them.

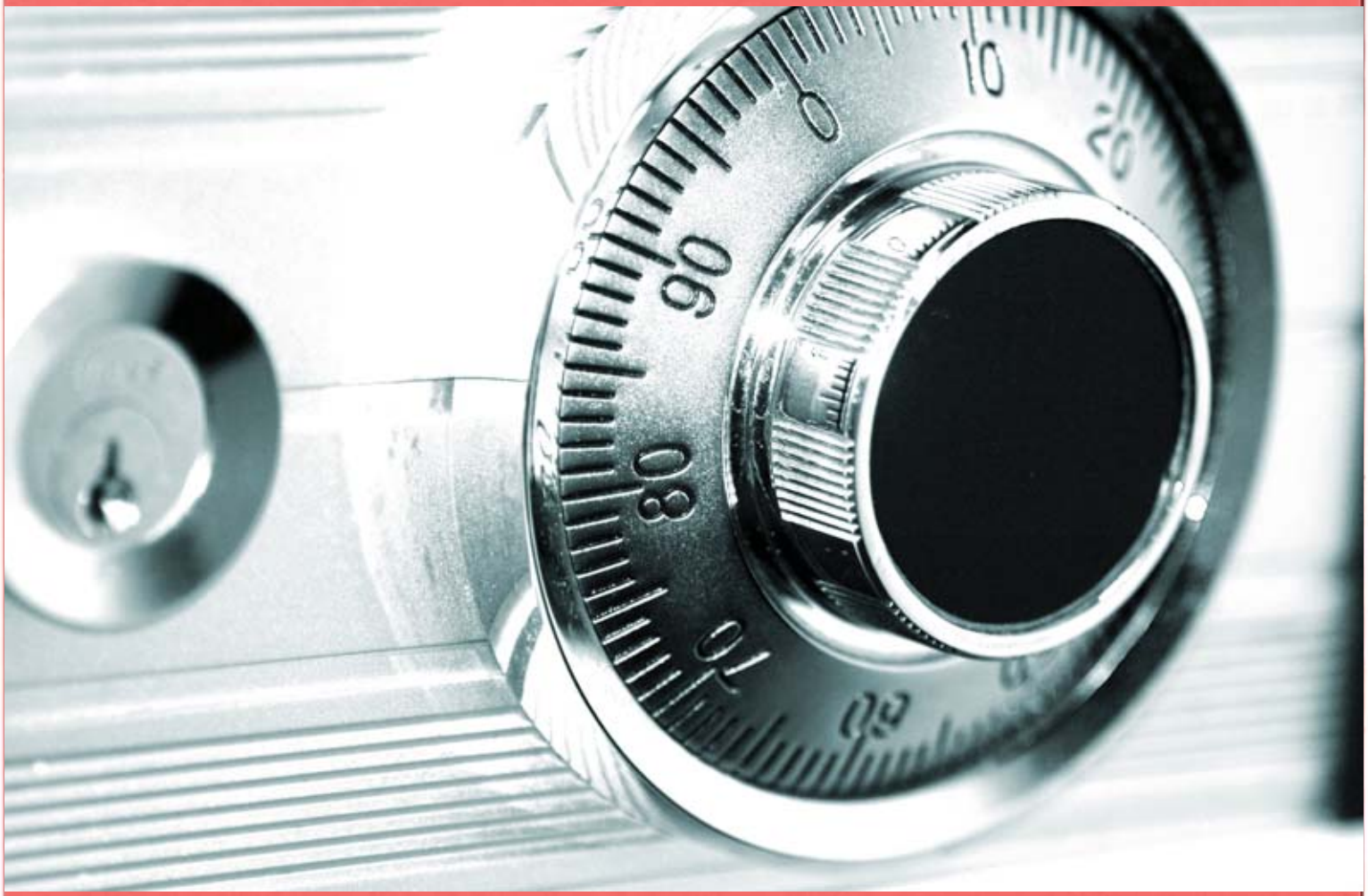
This might involve:

- Developing relationships with more than one business or supplier, so that if one is affected by an incident your business can continue as usual.
- Having backup processes in place for key business documents and information. Consider keeping copies of invoices, customer records, bank account details and insurance policies that are vital to your business. Locate this information at a second site and update it regularly.
- Plan for disruptions to electricity, gas, water, sewerage and telecommunications systems. Are backup systems available? Are there alternatives that can be used?
- Be prepared for broken machinery, damaged equipment and computer systems. Know who can fix them and have their contact details at hand.
- Think about having another site you could operate your business from.

Make checklists

- Good checklists can help you work out the most important actions that need to be taken.

Good security planning will be good for you, your business and your staff.



Make security planning part of your everyday business

Good security planning is good business.

It will help you manage and recover from all types of incidents. Security planning will deliver many practical benefits, such as:

- Contributing to the success of your business.
- Helping achieve your goals and objectives.
- Protecting the safety of you and your staff.
- Protecting your profitability and livelihood.

Consult with your employees about security planning and make security planning part of the way you do business.

National Counter-Terrorism Alert System

The National Counter-Terrorism Alert System communicates an assessed risk of terrorist threat to Australia. It dictates levels of precaution and vigilance individuals and organisations should apply to minimise the risk of a terrorist incident occurring. It is also the basis of public discussion of the risk of the terrorist threat to Australia.

Introduced in 2008, the National Counter-Terrorism Alert System is a flexible, tiered system which can be applied where necessary. It can cover the whole of Australia, specific states or territories, particular industry/business sectors, or geographic locations.

The Australian Government regularly reviews alert levels, based on ASIO assessments of the threat environment.

The Australian Government can change an alert level for one or more specific communities, locations or sectors. The flexible nature of the system reduces unnecessary disruptions to everyday life by avoiding impacts in communities, locations or sectors not affected by an assessed threat.

While the Alert System may not directly affect your day-to-day life, it is important that you are aware that these arrangements exist. All Australian governments are committed to ensuring that you can have confidence in Australia's ability to respond to any terrorist threat or activity.

For more information about the National Counter-Terrorism Alert System, please go to www.nationalsecurity.gov.au.

Australia has a four-level system of national counter-terrorism alert.

Low	terrorist attack is not expected	business as usual
Medium	terrorist attack could occur	business as normal, increased vigilance, making sure all business continuity/recovery plans are in place
High	terrorist attack is likely	review all business continuity/recovery plans, consider deploying additional security resources, pay attention to any official announcements about the threat
Extreme	terrorist attack is imminent or has occurred	pay attention to messages and instructions from national and local authorities, activate plans as necessary

Updates on the National Counter-Terrorism Alert Level are available at: www.nationalsecurity.gov.au.

More information

Emergency Services

In the event of an emergency – dial 000

Police – call your local police to receive general advice about security and safety issues in your area.

National Security

National Security Hotline – 1800 123 400

National Security website – www.nationalsecurity.gov.au

The Trusted Information Sharing Network website – www.tisn.gov.au

Risk Management and Business Continuity Standards

Standards Australia website – www.standards.org.au

Pandemic Preparedness

www.health.gov.au

www.dfat.gov.au

www.industry.gov.au

www.pmc.gov.au

ISBN: 1 921241 02 0

Published by the Australian Government Attorney-General's Department.

For other business information go to www.business.gov.au.

Australian Government

Attorney-General's Department