Government of **Western Australia**
Department of **Commerce**
Consumer Protection

Mandatory CPD 2016

Real Estate Agents and Sales Representatives

Distance Learning Participant Manual

Case Study: Commercial Focus

- Cybercrime and identity fraud
- Changes to foreign investment legislation in Australia

Government of Western Australia
Department of Commerce
Consumer Protection

IMPORTANT

This workbook and the accompanying presentation have been prepared for educational purposes only, as part of the **Department of Commerce Compulsory Professional Development Program**.

It is not, and should not be construed as, legal advice.

Any person in doubt as to their legal rights and obligations should seek the advice of a suitably qualified and competent legal practitioner.

Published by:	Department of Commerce
Developed by:	WCPT
Reviewed by:	TBA
First Published:	TBA
Version Number:	v1.0

Contents

Introduction

The purpose of this case study is to train commercial licensees and sales representatives in identifying risk within their agencies. We will explore two contemporary risk areas:

1. The occurrence of cyber-crime and identity fraud; and,
2. Changes that have recently been enacted by the federal government relating to foreign investment in real estate in Australia.

The case studies have been built using a blend of real estate industry examples and risk management trends. However, attendees must realise that risk management is an inherently unstable area of business. It is critical that attendees take the information contained within the case studies as an introduction to the subject matter, and seek to extend their awareness of the issues raised.

Instructions

1. Complete this mandatory distance learning pack by reading this book and answering the questions as you go. These questions will help you test your understanding and knowledge. **This book is yours to keep!**
2. When you have finished the reading and writing in this book, you are required to **complete the 14 question Evaluation Exercise and return it for marking**.

Did you know…

Even though the case studies created in this document are current and represent legitimate threats to agency security, the risk landscape is constantly changing. Cyber-crime in particular is **constantly evolving.** What does this mean? Each of us must continue to educate themselves, keep our security practices up to date and maintain an awareness of evolving threats.

Case Study: Cyber Crime and Identity Fraud

Let's start with a story.

Cartwright Commercial is a large commercial agency that manages a number of shopping centres in and around the Perth residential area. Cartwright operates across a number of inner city offices, with the leaders within each office maintaining close working relationships. Cartwright's management believe it is this culture of communication and data sharing that allows the group to identify and pounce on new opportunities before the competition.

Cartwright is on a growth path and is proud of the productive working relationships the company maintains with commercial tenants. That is, until the unthinkable happens.

Cartwright Commercial is contacted by one of their shopping centre tenants; the tenant advises that they have been hit by a ransomware attack and they are aware that another tenant within the centre had experienced the same thing. Cartwright staff consider this to be highly frustrating and a bit odd, but cannot see that there is much that they can do about it. But then another tenant reports that ransomware has locked their computer – and then another.

This is the tipping point for Cartwright tenants at this shopping centre, who meet to discuss the fact that something about the centre is clearly not secure. They demand to know how Cartwright has stored their information and accuse the company of sloppy security practices that have exposed tenant data.

Cartwright are in damage control. But when the company fails to respond immediately, the group of tenants get a local TV station involved and demand that Cartwright pays the damages associated with the data breach.

Amid the chaos, administration officer Kaelee starts to get a very uncomfortable feeling in her stomach. Two weeks ago, she had been contacted by a tenant who provided their name, date of birth and email address as proof of identity, and then asked if they could clarify some bank details due to some strange transaction activity. It had been a phone call from a charming tenant and she had thought nothing of it – but now that this incident of cyber-crime had come to light, Kaelee fears this could have been an instance of identity fraud at work. She is terrified to tell Cartwright's CEO that there might be more bad news…

Group Discussion

1. Summarise the problems that Cartwright Commercial is facing.

Here's a thought

Think about the immediate issues of crime and fraud, as well as impending customer service and reputation issues.

2. Who has been potentially impacted by the events that have unfolded at Cartwright Commercial?

Here's a thought

There could be an impact to staff, customers, contractors – even Cartwright's own business partners and providers.

3. Does the uptake of new technology unavoidably expose agencies to new risks?

Here's a thought

When we say no to technology, we say no to opportunity. So we need to manage the risk of technology, not run from it.

Introduction to Risk

Businesses of every size are exposed to risk every day. Let’s refresh the concepts of Risk, Threat and Risk Management.

What is risk?

Risk is defined by the International Organisation for Standardisation (ISO) as:

The effect of uncertainty on objectives.

Effect: a deviation from the expected.

Uncertainty: the state of deficiency of information related to an event, its likelihood and its consequence.

Objectives: in a business context, objectives could be related to financial success, health and safety or the environment.

Adapted from ISO Guide 73:2009 (en) Risk management – Vocabulary – Guides for use in standards

In other words, risk is what we didn’t see coming.

Although the definition of risk may be clear at a conceptual level, it can be difficult to articulate exactly how risk can impact ourselves, our staff, our businesses and our clients.

A simple way to make risk tangible is as follows:

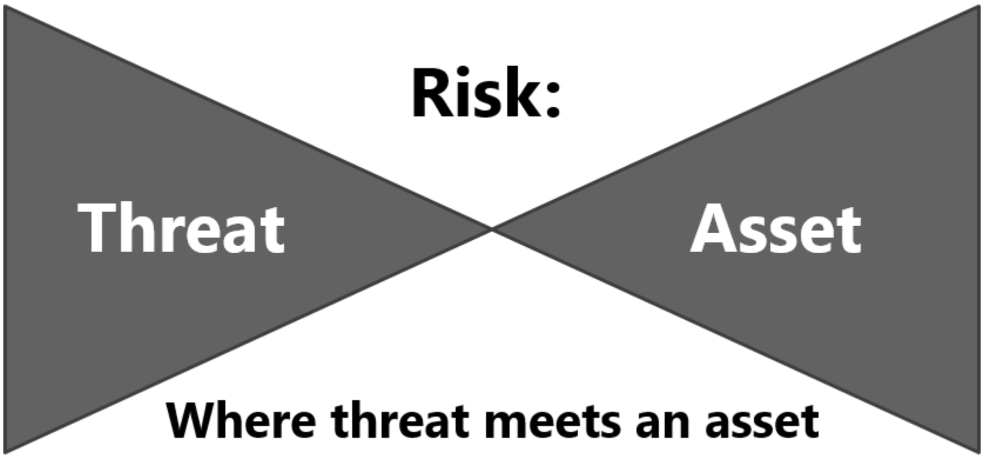


Figure 1: Risk Explained

A **threat** can be understood as either a mode of threat (such as a cyber-attack, a legislative oversight, or an environmental disaster), or a threat actor (an individual or group with an intent to cause harm). Threat modes are measured by likelihood and consequence, and threat actors are measured by intent and capability.

An **asset** doesn’t need to be physical: it may be your staff, reputation, intellectual property, your business premises or IT infrastructure – or the properties owned by your clients.

Questions

4. Where does risk come from in a business?

Did you know…

There is a 'known unknown' nature to risk. We know that changing technology, crime and complex processes give rise to risk, but we do not always know when, where, or how.

5. How do we separate risk from threat?

Here's a thought…

Threats cannot be stopped – but we can introduce measures to reduce risk.

6. Who is responsible for identifying and managing risk in a real estate context?

Here's a thought…

Should every member of an office team be responsible for managing and implementing risk management strategies? And can we really protect against everything?

Risk Management

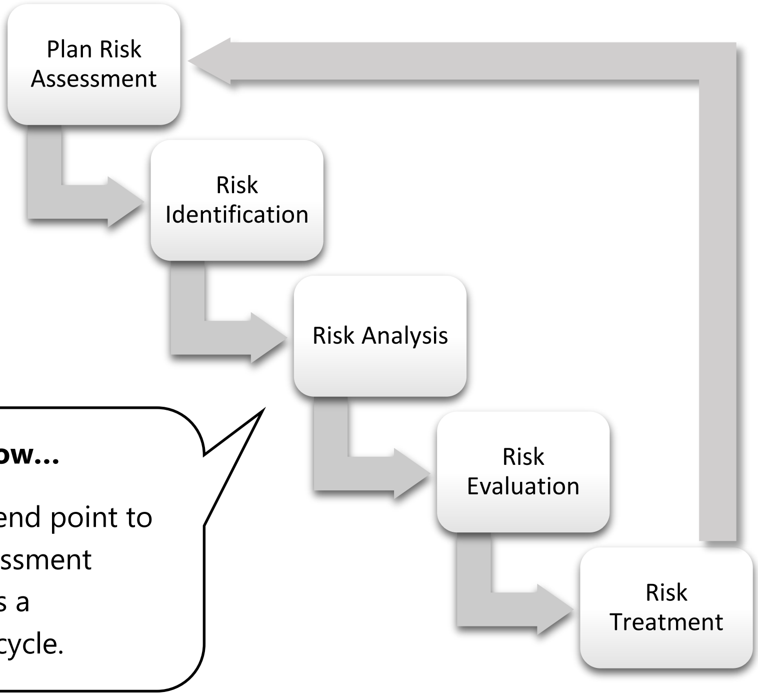
Risk management is about acknowledging that risk exists and finding a way to work around it. Effective risk management will minimise the impact of risk on a business – in fact, high performing business leaders are often able to create a competitive advantage by proactively and effectively managing risk.

What is Risk Management?

> Risk Management is defined by the International Organisation for Standardisation (ISO) as:
>
> **The coordinated activities to direct and control an organisation with regard to risk.**
>
> This coordination would likely be achieved through the use of a risk management policy and plan.
>
> Risk Management Policy: a statement of the overall intentions and direction of an organisation with regards to risk management.
>
> Risk Management Plan: a scheme specifying the approach and resources to be applied in the management of risk. This will include procedures and practices, accountability and responsibility, and timing of activities.
>
> *Adapted from ISO Guide 73:2009 (en) Risk management – Vocabulary – Guides for use in standards*

In other words, familiarising ourselves with the unknown and making sure we are ready for it.

The Risk Assessment Process



Did you know...

There is no end point to the risk assessment process – it's a continuous cycle.

Figure 2: The Risk Assessment Process

This process is explained in more detail below:

Plan Risk Assessment	- A business will first plan to conduct a formal risk assessment. - It may occur annually or twice annually, or even more often. - Assessment owners are identified: who will conduct the assessment and who oversees the process?
Risk Identification	- Involves the identification of risk source, risk event, risk cause and risk consequence. - Involves a thorough understanding of the threat landscape and organisational assets. - The necessary information may be gathered by consulting historical data, experts and staff.
Risk Analysis	- This is a formal process to determine the level of risk. - All identified risks are compared. - The analysis involves understanding the likelihood of something happening (or the exposure of the organisation to the risk), and the consequence should the risk be realised (monetary or otherwise).
Risk Evaluation	- This process ascribes a value to the risk that allows all risks identified to be ranked in order of impact and therefore importance. - A matrix is used to display the risks, which is achieved by defining ranges for consequence and likelihood. - This process will also consider an organisation's risk appetite – the amount of risk they feel comfortable with.
Risk Treatment	- This step involves a process to modify the risk. It may include avoiding certain activities, changing policies or processes, removing the risk source or taking steps to lower the impact or consequence of the risk. - Organisations will aim to mitigate or eliminate risks that produce wholly negative consequences.

Figure 3: The Risk Assessment Process in Detail

The process described above is then repeated at scheduled intervals, as organisations assess how their treatments have managed the risks previously identified, and determine whether there are new risks to be added to the list.

Case Study: More Detail

Cartwright Commercial do some research to get to the bottom of the incidents that have so significantly impacted their business.

Malware

- The agency is the common thread in this scenario. Unfortunately, Cartwright Commercial has been the target of a malware attack, which then had a secondary target of stripping and saving personal details that were stored on the exploited Cartwright system.
- The malware appeared to gain access to the computer when an employee clicked on some advertising on a webpage, while doing a spot of online shopping over a lunch break. The malware executed when the link was clicked, and was silently downloaded in the background. The malware was able to make its way onto other networked computers within the office.
- The malicious software in the head office had been identified when the antivirus software that runs on the system had been reactivated. Apparently, a staff member had disabled the antivirus software prior to a software update.

Ransomware

- Investigations reveal that a dodgy email was sent to addresses gathered from the Cartwright system. The ransomware was activated on the tenant computers when a link was clicked within this dodgy email. The email was purporting to offer an unbeatable OHS audit and implementation plan. Once the link was clicked, the ransomware managed to encrypt the computer using the same technology that encryption programs use to protect information – but in this case, it was to restrict access until payment was made.
- Cartwright Commercial contacted the police, who were unable to provide assistance. The tenant computer systems were in varying states of backup – many of them thought they had no option but to pay the ransom in order to regain access to their own client data. Others spent a lot of money on IT assistance to restore their systems following the attacks.

Threat Mode: Cyber-Attacks for Data Breach

Cyber-attacks that seek to obtain data for nefarious (dodgy) use come in many forms: malware and ransomware are two methods of attack.

Malware

Malware, or malicious software, is software that is designed to do damage to computer software.

Malware can take many forms and can be used to achieve many outcomes for a prospective hacker.

Research by Verizon suggests 5 malware attacks occur globally every second.

Ransomware

Ransomware is a type of malware that locks data and demands that the owner of the data make a payment to have the data unlocked. The payment amounts demanded can vary, but generally ransomware hacks are sent out in significant quantities and the payment amount is low to convince a user it may just be easier to make the payment ($500, for example).

Entities looking to prosper and profit via a malicious software attack do not discriminate based on industry or profession: every computer is a target, and usually, the metaphorical door to this data is unlocked and opened by the system's user.

Verizon research has found an average of 23% of phishing recipients open the email messages: 11% click on the attachments.

Social Engineering

A significant proportion of malicious cyber-attacks are achieved using some version of social engineering: that is, tricking a human to grant access to an illegitimate entity.

Phishing emails that trick people into providing sensitive information is a common tactic. Research by Verizon in 2015 has found an average of 23% of phishing recipients open the email message and a further 11% click on the attachments or links.

A further Verizon study has indicated that over 50% of phishing email opening occurs within an hour of the suspect emails landing in an inbox.

Threat Mode: Identity Theft

According to the ACCC, over 40% of phishing scams occur over the phone.

Identity theft is a type of fraud that involves using someone else's personal identification details to gain access to money or other benefits.

Social engineering is one of the most common ways to accomplish a theft of identity. Although we often consider email to be the primary danger zone for phishing activity, the phone is in fact the primary method for 'phishing' for personal details. In 2015, the ACCC suggested over 40% of phishing occurred via phone, whereas email represented 24% of efforts and SMS only 3%. And bear in mind - according to research by Verizon, "in 70% of attacks where we know the motive for the attack, there's a secondary victim".

Code of Conduct

9. Standard of service

An agent must exercise due skill, care and diligence.

10. Duties as to details of the transaction

(4) Without limiting the generality of subsection (1), an ag practicable after receiving instructions to act for a person in arranging a disposal, by way of sale, exchange or otherwise, of real estate and before a contract for that disposal is executed, make all reasonable efforts to verify —

(a) the identity of each person who claims to be, or to act for, a person who is to dispose of all or any of the real estate; and

(b) each person's authority to dispose of the real estate, or to act for the person disposing of it, as the case requires.

Here's a thought…

If we are 'tricked' by a fraudster, does that excuse us from our responsibilities under the Code of Conduct?

Group Discussion

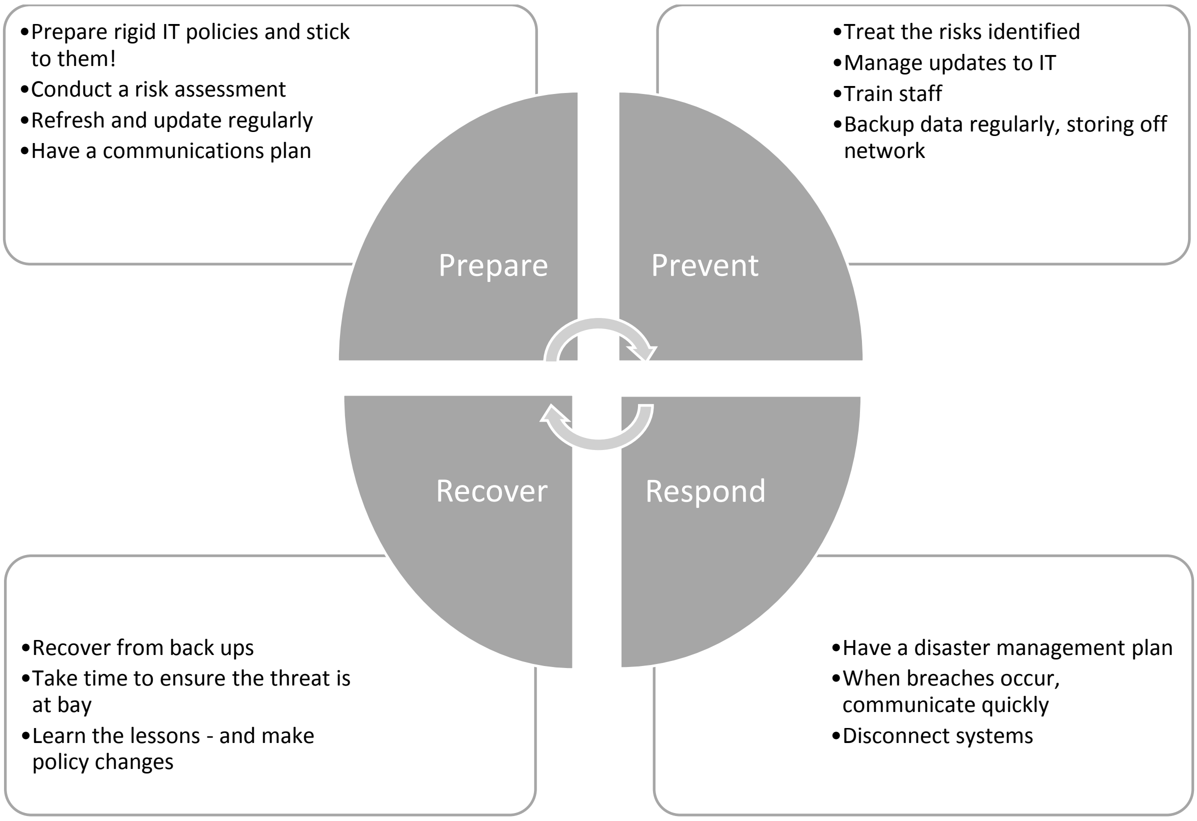
7. Discuss the relevance of the Code of Conduct in those instances where staff have been tricked into abandoning the usual security practices.

Managing Cyber and Identity Risk

The Risk Management process will assist real estate businesses in managing and mitigating the risks associated with cyber-attacks and identity theft. Given the propensity for such an attack to impact business, it is likely that Cartwright Commercial's licensee is now looking for a simple and rigid framework to guide his risk management efforts.

The PPRR Framework

New technology and evolving threat modes mean cyber and identity theft risks are changing all the time. This means our risk management approaches must continually evolve to keep up. This diagram provides a clear plan for organisations in managing risk. First, organisations must take ongoing and evolving steps to Prepare and Prevent. Then, in the case where a risk is realised, the Respond and Recover activities allow for a systematic and careful reaction.



- Prepare rigid IT policies and stick to them!
- Conduct a risk assessment
- Refresh and update regularly
- Have a communications plan

- Treat the risks identified
- Manage updates to IT
- Train staff
- Backup data regularly, storing off network

- Recover from back ups
- Take time to ensure the threat is at bay
- Learn the lessons - and make policy changes

- Have a disaster management plan
- When breaches occur, communicate quickly
- Disconnect systems

Figure 4: The Risk Assessment Process in Detail

The PPRR framework does not replace a risk assessment process – it adds an extra level of analysis and planning for those risks deemed to be of particular significance or impact to a business.

Using PPRR in our Cyber and Identity Theft Case

We will now use the PPRR model to assess how Cartwright Commercial could have improved their management of the issues identified.

Questions

8. Let's work backwards – assume the fraudulent behaviour was successful, but that Cartwright Commercial had comprehensive Respond and Recover actions in place. Under each heading, detail what these actions would have been, and what the impact on the business and its assets would have been.

Respond	Recover
Here's some thoughts to get you started: *Cartwright Commercial had thought about the worst case scenario and had a disaster recovery plan in place. This meant they were able to;* - … - … - …	*Cartwright Commercial were able to action the planning they had completed as part of ongoing risk management activities. This meant they were able to;* - … - … - …
Impact:	

Here's a thought…

Think about disaster recovery and reputation preservation.

9. Next – let’s consider the actions that may have significantly reduced the likelihood of the risks being realised – or, significantly reduced the impact. What actions should Cartwright Commercial have taken to Prepare and Prevent? Note the actions and summarise the impact on the business and its assets.

Prepare	**Prevent**
Here’s some thoughts to get you started: *Cartwright had completed a comprehensive risk assessment, which had allowed them to think about the types of cyber threats that might impact their operations. This meant they were able to;* - **…** - **…** - **…**	*Cartwright’s risk assessment allowed them to implement preventative measures to counter the threat of cyber-crime. These measures included:* - … - … - … **Here’s a thought…** This exercise is all about trying to familiarise yourself with the unknown.
Impact	

Summary

A significant number of cyber-attacks are enabled by a person. Awareness and education are therefore critical to managing cyber and identity-based fraud within a real estate business. Below are some key messages to communicate to teams and some tips to Prevent and Prepare within your business.

A watering-hole is a compromised legitimate website, frequented by a target user. In 2014, the Australian Cyber Security Agency handled more than 8100 watering-hole incidents.

1. **Work is for work**: computers connected to your office network should be used for work purposes. Personal use of a work computer exposes the system to unnecessary risk.
2. **Understand your privacy responsibilities**: The Privacy Act sets responsibilities for businesses, including how information is handled and what must occur in the event of a breach.
3. **Social media is a great tool for fraudsters**: an abundance of personal identifying detail is shared on social media, which could result in an accidental exposure to someone with malicious intent. To avoid this, delineate between those social media applications that will be used in a professional capacity versus those that are for personal use, and do not link them. Also be aware that contact details can be obtained via agency websites.
4. **Manage your mail**: use email filters to halt emails before they arrive in a user's inbox – limit the opportunity for users to accidently click on the link by removing access to possibly nasty emails altogether.
5. **Consider a whitelist**: for systems that store critical data (such as financial details or client identification details), consider a whitelisting approach. The opposite of blacklisting, whitelisting dictates the programs that are *allowed* to run on a system. If a piece of malware is not on the list, it will be unable to run – think of the protection offered to your trust accounting system.
6. **Build a culture of communication**: talk about trends and developments in cyber fraud. Seek feedback from staff and ensure they do not feel scared to raise a risk or a suspicious email or call. Have procedures to cross-check and question requests.
7. **Use sensible IT security measures**: keep passwords strong and up to date, use a firewall to counter remote intrusion and update your software as soon as updates become available and use an antivirus program that screens emails and attachments. In the event of a security breach, unplug and turn off your computer immediately.
8. **Assess and reassess your risks**: A risk management process is not a static activity to be conducted once a year. Undertake regular assessments to ensure you have a pulse on how risk within your agency has evolved.

Case Study Two: Foreign Investment in Australia

Cartwright Commercial has implemented some robust risk management practices around cyber-crime and identify theft. Let's check in with them.

Cartwright Commercial has experienced some hair raising times over the past six months. Nevertheless, the CEO has had support of the office licensees and staff in implementing a rigorous risk assessment and management program. With risks identified and mitigated, Cartwright have been able to reinstate trust with their tenants.

Cartwright continue to grow their business and have achieved significant success in the Perth commercial business. One area of growth is in assisting foreign investors to enter the Perth commercial property market, which is a business direction ripe with opportunity. However, given the impact that some external forces have had on his business recently, Cartwright's CEO is keen to make sure Cartwright "dot the i's and cross the t's" when it comes to their business conduct.

He asks Kaelee to do some research on Cartwright Commercial's obligations under Foreign Investment legislation. Is there anything they need to do, or is this a matter for investors only?

Group Discussion

10. What would be your advice to Kaelee? Where would you suggest she gather further information?

Here's a thought…

How do we make sure staff are empowered to make the right decisions to protect the agency, it's clients and it's interest?

> *“The Australian Government welcomes foreign investment. It has helped build Australia’s economy and will continue to enhance the wellbeing of Australians by supporting economic growth and prosperity.”*
>
> *Foreign Investment Review Board, 2015*

Why is foreign investment important to the Australian economy?

According to the Foreign Investment Review Board (FIRB), in 2013-14 financial year foreign investment in Australian commercial property was valued at almost $40 billion dollars. This high level of foreign investment drives employment, productivity growth, and innovation.

Foreign investment is regulated by the FIRB and the *Foreign Acquisitions and Takeovers Act 1975 (FATA)*. There are strict rules in place to ensure foreign investment is conducted in a lawful way. In 2015, the federal government announced a tightening of these laws. The changes include:

- Increasing the substantial interest threshold from 15% to 20%, so that it aligns with the threshold set out in Australia’s corporate takeover rules.

- Incorporating the existing rules relating to foreign investment in land currently set out in Australia’s Foreign Investment Policy (2015) into the *FATA* so they have legislative force.

- Introducing stricter penalties to make it easier to track foreign investors who breach the rules. Criminal penalties were increased to $135,000 or three years imprisonment for individuals and to $675,000 for companies; persons or organisations who assist those who break the rules will also be a target for penalties.

Changes to Foreign Investment Legislation

The Commonwealth government introduced changes to the *FATA* in order to strengthen the integrity of the foreign investment framework. The following table outlines the penalties for breaches of rules which apply to business or agriculture investments:

Breach of current rule	Proposed new penalties
Foreign person makes an acquisition without approval *(approval would normally have been granted)*	**Increased Criminal Penalty** Maximum criminal penalty of: Individual — 750 penalty units ($135,000) or 3 years imprisonment (Bill implies both could apply). Company — 3,750 penalty units ($675,000). **Civil penalty** Maximum civil penalty of: Individual — 250 penalty units ($ $45,000 (Company — 1,250 penalty units ($225,000)
Foreign person fails to comply with a condition of approval	**Increased Criminal Penalty** Maximum criminal penalty of Individual — 750 penalty units ($135,000) or 3 years imprisonment (or both). Company — 3,750 penalty units ($675,000). **Civil penalty** Maximum civil penalty of: Individual — 250 penalty units ($45,000) Company — 1,250 penalty units ($225,000)
Person assists foreign investor to breach rules	**Civil penalty** Maximum civil penalty, the same as the primary breach, of: Individual — 250 penalty units ($45,000)Company — 1,250 penalty units ($225,000) **Criminal Penalty** Knowingly assisting another person to commit a criminal offence is an offence under Section 11.2 of the Criminal Code (maximum penalty is the same as the primary offence).

Foreign investment threshold changes and application fees: Investment in business, commercial real estate and agricultural sectors:

Type of investor	Type of acquisition	Previous threshold	New threshold	Application Fee from 1 December 2015
Privately owned investors from FTA partner countries that have the higher threshold	Developed commercial real estate (including heritage-listed properties)	$1,094 million (indexed annually)	$1,094 million (indexed annually)	$25,000
	Vacant commercial land	$0	$0	$10,000
	Business acquisitions in non-sensitive sectors	$1,094 million (indexed annually)	$1,094 million (indexed annually)	$25,000 (or $100,000 for business acquisitions where the value of the transaction is greater than $1 billion) $10,000 if an internal reorganisation
	Business acquisitions in sensitive sectors	$252 million (indexed annually)	$252 million (indexed annually)	$25,000 (or $100,000 for business acquisitions where the value of the transaction is greater than $1 billion) $10,000 if an internal reorganisation
	Rural land	$1,094 million (indexed annually)	$1,094 million (indexed annually) for US, NZ and Chile. $15 million (cumulative) for China, Japan and Korea.	Rural land less than $1 million: $5,000
				Rural land equal to or greater than $1 million: $10,000, (then $10,000 incremental fee per additional $1 million in rural land value, capped at $100,000)
	Agribusinesses	$1,094 million (indexed annually)	$1,094 million (indexed annually) for US, NZ and Chile. $55 million (indexed annually) for China, Japan & Korea.	$25,000 (or $100,000 for agribusiness acquisitions where the value of the transaction is greater than $1 billion)

Privately owned investors from non-FTA countries and FTA countries that do not have the higher threshold	Developed commercial real estate	$55 million (indexed annually)	$55 million (indexed annually)	$25,000
	Heritage-listed developed commercial real estate	$5 million	$5 million	$25,000
	Vacant commercial land	$0	$0	$10,000
	Business acquisitions in (sensitive and non-sensitive sectors)	$252 million (indexed annually)	$252 million (indexed annually)	$25,000 (or $100,000 for business acquisitions where the value of the transaction is greater than $1 billion) $10,000 if an internal reorganisation
	Rural land	$252 million (indexed annually)	$15 million (cumulative)4 $50 million for Singapore and Thailand	Rural land less than $1 million: $5,000
				Rural land equal to or greater than $1 million: $10,000, (then $10,000 incremental fee per additional $1 million in rural land value, capped at $100,000)
	Agribusinesses	$252 million (indexed annually)	$55 million (indexed annually)	$25,000 (or $100,000 for agribusiness acquisitions where the value of the transaction is greater than $1 billion)
Foreign Government Investors	All direct investments (regardless of the sector)	$0	$0	Based on the applicable fee above.
	New business proposals	$0	$0	$10,000
	Interests in land (including rural land)	$0	$0	Based on the applicable fee above.

Source: http://jbh.ministers.treasury.gov.au/media-release/034-2015/

Case Study: More Detail

Of particular importance to licensees and sales representatives is the increased focus on penalising those individuals who assist foreign buyers in acquiring real estate assets illegally.

Questions

11. What should Cartwright Commercial do to make sure its obligations are met with respect to foreign investment legislation?

Here's a thought…

It is critical that Cartwright act in accordance with ***all*** legislation governing the activities of a real estate representative or agent. It should be further noted that, even if a licensee/sales representative does not commit an offence under the Act, they may still be liable to a client for breach of contract, negligence or misrepresentation under the *Australian Consumer Law* if they fail to advise foreign investors of the requirements of the Act.

12. Legislative change that is missed or ignored represents a significant threat mode for real estate professionals in Western Australia, with substantial potential consequences. What steps can be taken to Prepare, Prevent, Recover and Respond with respect to monitoring and complying with legislative change?

Here's a thought…

We can use risk management to ensure we keep a watchful eye on legislative change.

FAQs Relating to Foreign Investment

Q: I want to buy commercial land for development

A: Land for commercial development is vacant land which is available for commercial development and not to be used for residential purposes. Foreign persons need to apply to buy or take an interest in land for commercial development (including to start a forestry business), regardless of the value of the land. Proposed acquisitions of land for commercial development are normally approved subject to the condition that continuous construction commence within 5 years.

Q: I want to buy developed commercial real estate

A: Foreign persons need to apply to buy or take an interest in developed commercial real estate valued at $55 million or more – unless the real estate is heritage listed, then a $5 million threshold applies. Foreign government related entities are required to notify all acquisitions of developed commercial real estate, regardless of the value.

Q: I want to buy multiple use property which includes both commercial and residential properties.

Foreign persons need to apply to buy or take an interest in developed commercial real estate valued at $54 million or more - unless the real estate is heritage listed, then a $5 million threshold applies. Foreign government related entities are required to notify all acquisitions of developed commercial real estate, regardless of the value.

Developed commercial property includes hotels, motels, hostels and guesthouses, as well as individual dwellings that are a part of these properties. Buying a unit in a hotel that is owner-occupied or rented out privately (that is, it is not part of the hotel business) is considered to be residential property. As such properties may constitute an acquisition of residential real estate (for which there is no threshold for notifying) it is recommended that, if you are in any doubt, you lodge an application.

Source: FIRB

Note

The Department of Commerce has produced a Guidance Note entitled *Code of Conduct for agents and sales representatives: Client identification verification and real estate fraud prevention*. Attendees may find this Guidance Note helpful in understanding the application of the Code of Conduct to instances of fraud or identity theft. The Guidance Note can be accessed at the following address:

http://www.commerce.wa.gov.au/sites/default/files/atoms/files/guidancenotecodeofconductagentsandsalesrep.pdf

Sources

Australian Cyber Security Centre 2015, *ACSC Threat Report 2015.* Available from: https://acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf

Australian Signals Directorate 2015, *Application Whitelisting Explained*. Available from: http://www.asd.gov.au/publications/protect/application_whitelisting.htm

Foreign Investment Review Board 2015, *FIRB Annual Report 2013-14.* Available from: http://www.firb.gov.au/content/Publications/AnnualReports/2013-2014/_downloads/FIRB-AR-2013-14.pdf

Foreign Investment Review Board 2015, *Frequently Asked Questions*. Available from: http://www.firb.gov.au/content/faq.asp

Scam Watch 2015, *Phishing*. Available from: https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing

The Treasury 2015, *Government strengthens the foreign investment framework*. Available from: http://jbh.ministers.treasury.gov.au/media-release/034-2015/

Verizon 2015, *Verizon Data Breach Investigations Report 2015*. Available from: http://www.verizonenterprise.com/au/DBIR/2015/

Other Relevant Sites

Commerce website: www.commerce.wa.gov.au

WAScamNet website: www.scamnet.gov.au

Australian Cybercrime Online Reporting Network: www.acorn.gov.au

Stay Smart Online Alert Service: www.communications.gov.au/what-we-do/internet/stay-smart-online

Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

(UPDATED) AUGUST 2012

Application whitelisting explained

1. Application whitelisting is one of the top four strategies in DSD's list of *Strategies to Mitigate Targeted Cyber Intrusions*. This document provides high-level guidance on what application whitelisting is, what it isn't, and how Information Technology Security Advisers can apply it effectively in a Windows-based environment.

Why implement application whitelisting?

2. Application whitelisting is designed to protect against unauthorised and malicious programs executing on a computer. It aims to ensure that only specifically selected programs and software libraries (DLLs) can be executed, while all others are prevented from executing.

3. While primarily implemented to prevent the execution and spread of malicious software (malware), it can also prevent the installation or use of unauthorised software.

4. Implementing application whitelisting across an entire organisation can be a daunting undertaking, however deployment to high-value and often targeted employees such as executive officers and their assistants can be a valuable first step.

What is application whitelisting?

5. Application whitelisting comprises the following technical steps:

   a. identifying specific executables and software libraries which should be permitted to execute on a given system;

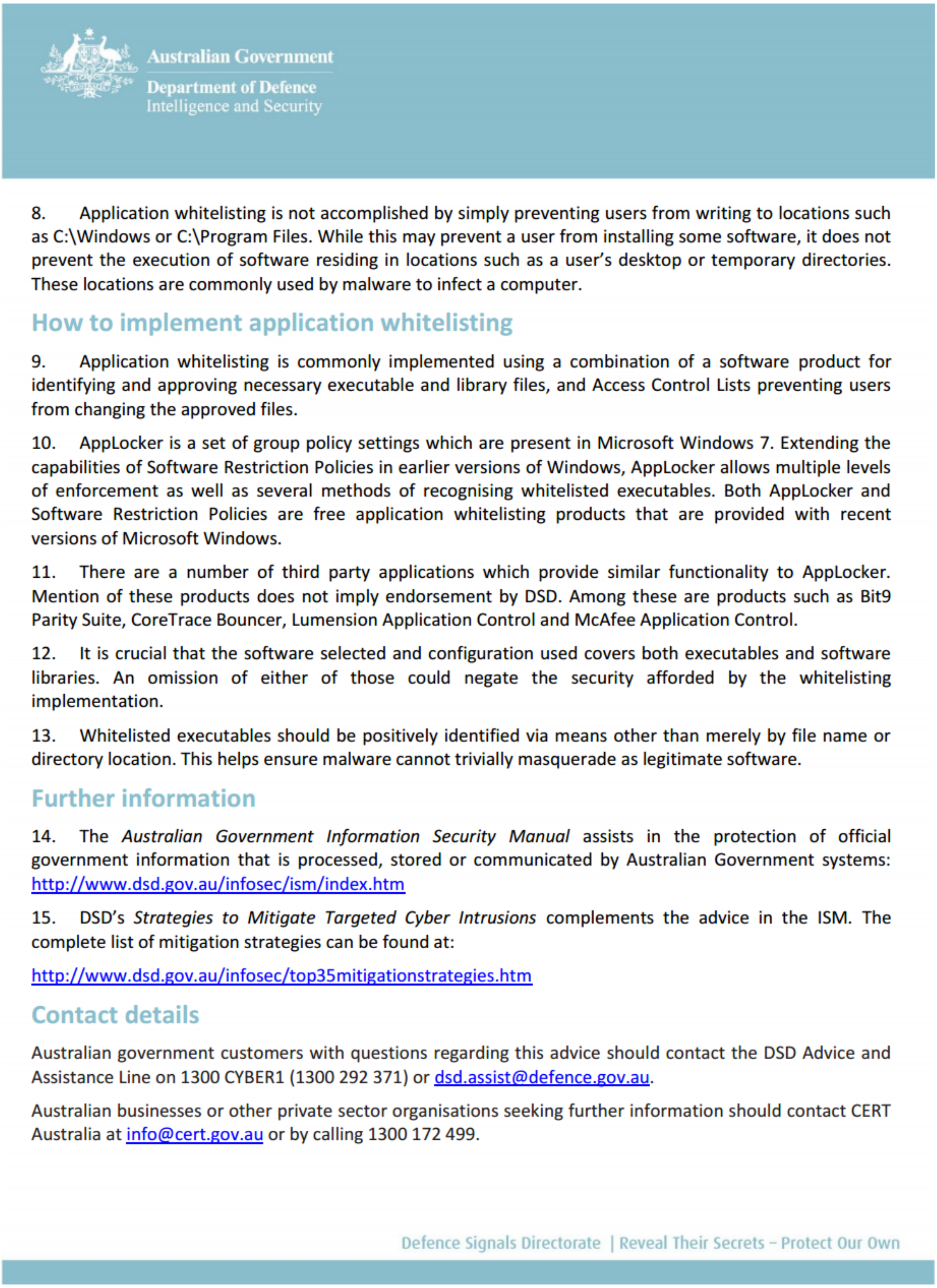
   b. preventing any other executables and software libraries from functioning on that system;

   c. preventing users from being able to change which files can be executed.

6. An intermediate approach to application whitelisting is identifying entire directories from which users are allowed to execute programs, such as C:\Windows, C:\Program Files, or even C:\Program Files\Specific Application. This provides some measure of protection from applications executing outside the specified directories but it does not take into account a number of possible scenarios for compromise. This technique is better than not applying application whitelisting at all, but a more comprehensive approach should be considered at the earliest opportunity such as at the next Standard Operating Environment (SOE) refresh.

What application whitelisting is not

7. Providing a portal or other means of installation of only approved software is not application whitelisting. This does not prevent users from running software not listed on the portal, and will not prevent malware from executing and compromising a system.



Australian Government
Department of Defence
Intelligence and Security

8. Application whitelisting is not accomplished by simply preventing users from writing to locations such as C:\Windows or C:\Program Files. While this may prevent a user from installing some software, it does not prevent the execution of software residing in locations such as a user's desktop or temporary directories. These locations are commonly used by malware to infect a computer.

How to implement application whitelisting

9. Application whitelisting is commonly implemented using a combination of a software product for identifying and approving necessary executable and library files, and Access Control Lists preventing users from changing the approved files.

10. AppLocker is a set of group policy settings which are present in Microsoft Windows 7. Extending the capabilities of Software Restriction Policies in earlier versions of Windows, AppLocker allows multiple levels of enforcement as well as several methods of recognising whitelisted executables. Both AppLocker and Software Restriction Policies are free application whitelisting products that are provided with recent versions of Microsoft Windows.

11. There are a number of third party applications which provide similar functionality to AppLocker. Mention of these products does not imply endorsement by DSD. Among these are products such as Bit9 Parity Suite, CoreTrace Bouncer, Lumension Application Control and McAfee Application Control.

12. It is crucial that the software selected and configuration used covers both executables and software libraries. An omission of either of those could negate the security afforded by the whitelisting implementation.

13. Whitelisted executables should be positively identified via means other than merely by file name or directory location. This helps ensure malware cannot trivially masquerade as legitimate software.

Further information

14. The *Australian Government Information Security Manual* assists in the protection of official government information that is processed, stored or communicated by Australian Government systems: http://www.dsd.gov.au/infosec/ism/index.htm

15. DSD's *Strategies to Mitigate Targeted Cyber Intrusions* complements the advice in the ISM. The complete list of mitigation strategies can be found at:

http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

Contact details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.

Defence Signals Directorate | Reveal Their Secrets – Protect Our Own

Available from: http://www.asd.gov.au/publications/protect/application_whitelisting.htm