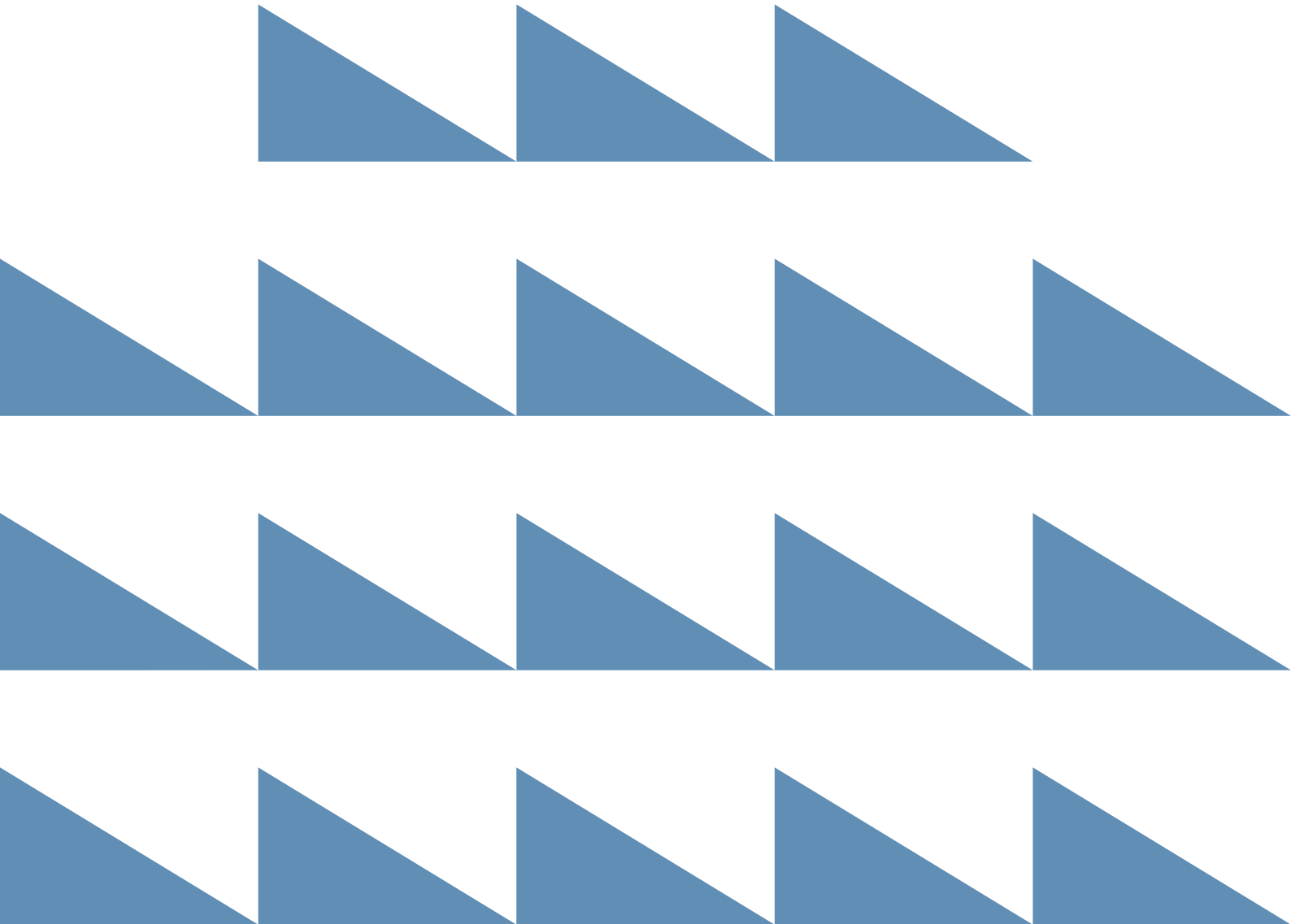
ibac independent broad-based anti-corruption commission
Victoria

A guide for preventing unauthorised disclosure of information

May 2015



This guide is for public sector agencies, to help prevent or mitigate the threat of agency staff disclosing information without authority or misusing information gained in their official capacity. It provides strategies to reduce the risk of public sector employees becoming targets due to their access to valuable information.

Public bodies may not be aware of the threats posed by individuals or groups targeting their employees for the purpose of some personal gain. This is reflected in the absence of prevention and detection measures in place to mitigate this threat. Limited appreciation or understanding of the threat means that instances of cultivation are more likely to occur, remain unreported and result in widespread and long-term damage to the public sector. Increasing public sector employees' awareness of the threat and highlighting key prevention and detection measures are effective ways to address this issue.

Background

Growing public concern over the security and privacy of their information held by public sector agencies has seen a strengthening of regulations designed to protect confidentiality and guard against fraud and identity theft. Measures including firewalls, anti-virus software, biometrics and identity access badges have made agencies more effective at blocking threats from the outside.

Such technologies are largely passive in approach however, designed to thwart a direct attack and provide only a first line of defence.

Evidence is growing for a trend toward small, targeted attacks – possible only with agreed or unintended cooperation of agency insiders. Ignoring such internal dangers over prioritisation of external threats can leave an agency extremely vulnerable.

A survey of security event data from Australian organisations with information security functions, received responses from over 50 government agencies acknowledging the identification of a threat or occurrence of a breach. Of these, 45 per cent involved both internal and external perpetrators and a further 27 per cent involved internal threats alone.

Damage from unauthorised disclosure of information by insiders carries the potential to significantly rival or even exceed the damage caused by other means such as external 'hacking'. As a trusted employee, they carry valid authorisation and will typically have unchallenged presence, movement and access within an organisation's systems and information holdings. Also, insider threats can be more difficult to detect than attempts to attack from the outside.

Public bodies and their employees can also be targeted by others to access:

- sensitive information or systems
- decision-making processes, matrices or criteria
- property or goods with a high resale value
- knowledge that facilitates criminal activity.

The means by which a perpetrator can access public sector information, decision-making processes or commodities are varied and can include technology-based infiltration or unauthorised physical access (breaking and entering). However, most would lack the capabilities to launch large-scale electronic attacks on public bodies. Also, the physical security measures in place at public bodies' locations may discourage attempts at physical access or prevent ongoing access.

In such an environment, the cultivation of public servants represents an attractive and easier way to access the information, systems, decision-making processes or commodities held by public bodies. Where a public servant can be persuaded to cooperate with an individual or group with criminal intent, they offer ongoing access while employing their inside knowledge of the public bodies' systems to avoid detection.

Consequences

When a public sector employee has been successfully cultivated, there are significant ramifications for the individual, their public body and society more broadly.

Employees	Public body	Society
• embarrassment • physical harm • threats to self, family and friends • loss of emloyment	• reputational damage • financial loss • loss of intellectual property • damage to another's privacy • breach to physical security • imtimidation, violence and threats to employees	• threat to safety of community members • exploitation of personal information • loss of services or provision of inadequate services • unfair tendering conditions • loss of confidence in public organisations

Where agencies lack prevention and detection measures to address these threats, significant damage can be done over a long period of time.

Targets

Information

Public servants have access to information valuable to the commission of serious crime. This information can assist to identify criminal opportunities, facilitate criminal activity, undermine competitors or avoid detection.

Information can be directly used for criminal activities. For example, identity information is particularly valuable as it facilitates identity fraud, debt collection, witness intimidation, extortion, or can be sold to other criminal groups.

Some agencies with access to sensitive information are often not aware of the risks presented by criminal groups and lack basic protections against cultivation.

Law enforcement or regulatory information is also attractive, allowing crime groups to avoid detection. This might include details of individual criminal records, law enforcement intelligence, or law enforcement methodologies and targeting priorities.

Databases managed by police and road authorities represent the largest and most comprehensive sources of identity information within the public sector. An increasing number of public sector bodies also collect identity information and could potentially be targeted. Information such as transport card registration details, ratepayer lists and animal registration databases hold valuable identity material that could be used for criminal purposes.

Decision-making and regulatory processes undertaken by public servants could also be targeted. The construction, planning, development, prostitution, gaming and liquor industries present attractive opportunities to engage in illegal or semi-legal practices for profit or to launder proceeds of crime. Regulators overseeing these industries are attractive targets for those seeking to increase their profits or avoid detection.

Work areas

It is not only sensitive operational areas that could be targeted. Although the focus has traditionally been on 'front-line' operational staff, support officers in administrative, data entry and information technology areas may also be in a position to access sensitive information or conceal improper actions.

No public body is immune from being targeted and potentially penetrated by organised crime.

In determining which work areas face the highest risk of cultivation attempts, public bodies should consider for each work area:

- what information, decision-making powers and commodities are accessible
- employee demographics (who)
- formal and informal work practices and security practices (where and how).

Poor protective security and management processes have been consistently identified in cases where government insiders have worked in concert for organised criminal groups.

Factors that have been associated with exploited work areas include:

- a poor security culture
- poor proactive use of auditing functions
- a lack of adequate, role-based, personnel security risk assessment
- poor pre-employment screening
- poor communication between business areas
- a lack of awareness of personnel-related risks at a senior level
- inadequate corporate governance
- general workplace dysfunction.

Tail gating[1] and shoulder surfing[2] also provide unauthorised access to secured areas or to information that is observable in a public place.

[1] Seeking entry to a restricted area by walking closely behind a person who has legitimate access.

[2] Observing private information over the shoulder of an employee in a public place such as public transport, airport or coffee shop.

In addition to these internal factors, public bodies must also consider how they share their information and systems. Although a public body may have identified high-risk work areas internally, they may remain vulnerable where information and access to systems are shared with other bodies. Multi-agency working groups and shared databases can bring together employees with different levels of vetting, training, oversight, values and understanding of corruption risks.

These discrepancies can be even more likely where public bodies outsource any functions to private providers or engage temporary staff or contractors. In such cases, bodies that observe best practice around their permanent staff or internal functions may still leave themselves vulnerable.

Vulnerable individuals

Some information users in a public sector organisation are more likely targets, including:

- senior executives and their assistants
- help desk staff, system and network administrators, users who have administrative privileges to operating systems or applications such as databases
- all users who have access to sensitive information, including information which could provide an individual, group or even foreign government with a strategic or economic advantage such as pricing, sales or tender information
- users with remote access
- users whose job role involves interacting with unsolicited emails from members of the public and other unknown internet users.

Certain personal and environmental factors are associated with those public sector employees most vulnerable to cultivation.

Although not all individuals with one or all of these indicators will be vulnerable to an approach, they are reliable risk indicators that supervisors, security managers and human resources personnel should be aware of.

Personality factors are those innate characteristics of an individual relating to how they respond to situations and interact with others. Factors identified as being associated with a public sector employee's susceptibility to cultivation include:

- immaturity (including a lack of life experience and naïveté)
- having low self-esteem (extremely dependent on recognition, struggles to cope with adversity)
- being amoral and unethical (lacking moral values or personal integrity, shows no remorse)
- being superficial (lacking a sense of identity)
- being prone to fantasising (believing they are engaged in activities that have no basis in reality)
- impulsivity (seeking instant gratification and does whatever feels good in the moment)
- lacking conscientiousness (ignoring rules, duties and obligations, showing a lack of focus)
- being manipulative (using others to serve their own self-interest)
- being emotionally unstable (prone to exaggerated mood swings and overreacting to problems)
- showing evidence of psychological or personality disorders
- spreading mischievous, vexatious or defamatory comments about the organisation
- having preferred alignment with interest groups that have values and agendas different to the employing organisation.

Environmental factors include negative life events or lifestyle factors that increase individuals' vulnerabilities. These can include serious financial, alcohol, gambling or drug problems, loss of status at work, significant personal injury, death of a family member or close friend, relationship break-ups or loneliness.

In cases identified to date, these factors have left public sector employees vulnerable to opportunistic approaches from criminal groups. Proactive targeting of individuals with these characteristics is being undertaken by sophisticated organised crime groups interstate and overseas. The most sophisticated have demonstrated a capacity to evolve quickly and to learn from crime groups in other jurisdictions and could adopt similar strategies targeting Victorian public sector employees in the future.

Cultivation strategies

Pre-existing relationships

Motivated individuals or groups will exploit family relationships, intimate partnerships, pre-existing friendships and cultural links to gain access to public bodies' information and systems. Such loyalties and social bonds can be enduring and enable corruption.

Pre-existing relationships present a particularly powerful opportunity in regional areas. The greater levels of social connectivity that exist in smaller regional areas increases the likelihood of criminals in these areas knowing public sector employees.

Long-term relationships, particularly those based on bonds of family, friendship or culture can lead to a shift in public sector employees' loyalties away from their employer's organisational values, standards or codes. Within such a relationship, a corrupt official can justify their actions by arguing that 'just helping a friend' is the 'right' thing to do, even where it involves a betrayal of the public trust.

Social media

Social media provides an additional environment in which criminals can engage with public sector employees. However unlike traditional 'real-world' forums, social media allows searching for employment details, personal interests and characteristics that could then identify personal vulnerabilities.

Social media allows large numbers of public sector employees to be identified including, in cases such as LinkedIn, their work units and responsibilities. When combined with information from other social media platforms, it is possible to gain access to names, dates of birth, photographs, details of their friends and families, personal interests, where they spend their spare time, gambling behaviour, relationship status and emotional state.

Many cases exist where criminals have used these details to initiate contact, which at first may appear to be innocent to the target, but then can be built upon to judge the potential for compromising the person being targeted or used to persuade a course of action. Organised crime groups across Australia are already using social media platforms in innovative ways, such as to recruit individuals to serve as couriers for illicit drugs and precursor chemicals. It is highly likely that Victorian crime groups will increasingly use social media to identify public sector employees and to cultivate relationships that facilitate corruption.

Social engineering

Social engineering, in the context of information security, refers to the psychological manipulation of people into performing actions or divulging confidential information. A type of 'confidence trick', social engineering techniques are based on known cognitive biases in human decision making, which are then exploited. The most common type of social engineering happens over the phone such as using an invented scenario, posing as a senior person or representing an organisation of authority. They can also be in person, via email, social media or by leaving other information as bait.

Infiltration

Public bodies should also be aware of the risk of people seeking employment in their organisation, with the specific aim of using their position to facilitate crime through access or unauthorised release of information.

Across Australia there have been some identified cases where organised crime groups have adopted a strategy of targeted penetration. However, Australian integrity agencies have consistently found that corrupt activity is most likely to occur after an individual has joined a public sector agency, rather than as a result of targeted infiltration.

Prevention and detection strategies

Create and maintain a security culture

The most effective protection against cultivation attempts is a robust security culture. When employees and management understand the threat through awareness raising, have received appropriate training and are kept up-to-date on emerging security issues, they are equipped to detect and repel approaches and to identify warning signs in others' behaviour. Promoting professional and corruption-resistant cultures within agencies addresses not only the threat of unauthorised information release, but encourages resistance to a range of other corruption risks. A security-aware culture is maintained in any organisation by regularly reinforcing the standard by which everyone operates. These standards should be applied across permanent employees, contractors, temporary staff and regardless of length of employment or seniority within the organisation.

Conduct risk assessments and plan mitigations

The risks associated with insider threats should be addressed in organisational risk assessments. When framing risk assessments, public bodies might consider:

- the current security environment: Are there many security incidents? Are there good levels of detection or self-reporting? How are incidents dealt with? What don't you know?
- high-value information and systems: What information or systems controlled by a public body would be valuable to an organised crime group? Who has access? Who is vulnerable? Who is motivated?
- precedence: Has a public body or similar bodies been targeted? How was this achieved? Did it work?

The functional areas of greatest risk will be different across different bodies, meaning there is not a uniform set of mitigation strategies that should be applied to all public bodies.

Organisational risk assessments should also acknowledge that some work areas or positions within the one body are at higher risk and should be subject to additional security measures.

Conduct vetting and regular revalidation of employees

Screening employees serves as both a prevention and detection strategy against cultivation. Vetting involves a series of checks to ensure individuals entrusted with access to information or resources are suitable and can be relied upon to safeguard them. Vetting employees when they are recruited increases the likelihood that targeted infiltration attempts will be identified. It also helps identify employees with risk factors that might make them vulnerable to targeting in the future, providing public bodies an opportunity to put risk mitigation strategies in place.

Although pre-employment screening is important, it will not identify all individuals who present a security risk. Vulnerabilities such as personality factors, lifestyle changes or workplace behaviours are not always observable at recruitment or may only arise following recruitment. Revalidation of employees' security clearances at regular or random intervals during their employment ensures that public bodies can respond to changes in an employees' risk profile.

Revalidation is particularly important as it appears more likely that criminals will target existing employees rather than try to infiltrate agencies. A system of revalidation also acknowledges that employees' access and influence within a public body will generally increase the longer they have been employed, increasing their potential value to others.

Regular auditing

One of the most effective means of identifying incidents of cultivation of public sector employees is proactive and random auditing. Routine auditing can identify where there has been inappropriate access, use or sharing of information, systems or property after an incident. Prevention involves proactive and random auditing to identify 'red flags' and patterns of interaction which then provides an opportunity for intervention or mitigation prior to a damaging event occurring.

Establish a declarable associations process

Personal relationships between public sector employees and criminal entities have long been identified by anti-corruption bodies as a corruption risk. These relationships have the potential to facilitate the inappropriate release of information, compromise law enforcement activities or facilitate criminal activity. Such associations could be perceived as influencing a public sector employee's capacity to perform their role. The risks posed by such associations can be categorised as potential, actual or perceived.

In some cases, associations between public sector employees and individuals engaged in criminal activities are unavoidable. These associations might arise through family links, clubs, societies, secondary employment or social activities. Consequently, they should be addressed by being declared to an employer so that risk can be appropriately managed. Managing these risks also protects an employee from rumour or detrimental action due to others' perceptions of the relationship.

It is important to note that having a declarable association is not, in itself, misconduct. The improper act stems from a failure to declare or properly manage the association. It is for this reason that such associations are best referred to as 'declarable' rather than 'inappropriate' associations.

Declaring associations helps maintain the credibility of an employee and the public body as a whole and reduces risks to a public body's operational integrity.

Agencies should have clear policies in place around the identification and reporting of declarable associations. Where employees do not have a clear understanding of what constitutes a declarable association or how they should declare that association, compliance with the policy is likely to be poor.

Best practice policies integrate mandatory reporting of declarable associations into the recruitment process and during periodic checks on employees' personal particulars.

Public bodies should provide clear policies around declarable associations with a structured and centralised system of recording such associations. The very act of declaring an association can reduce risk by making both the employee and their manager conscious of potential conflicts of interest associated with a relationship. However, much of the preventative value of a declaration is lost if it is not accurately recorded in a way that can support decision making in the future. For example, if an organised crime figure is befriending multiple employees across different areas of an organisation, this might not be identified if declarable associations are not centrally recorded.

Staff welfare

Many of the issues that heighten employees' susceptibility to organised crime cultivation can also have adverse impacts on their welfare. Organisational responses to illicit drug use, problem gambling and relationship breakdowns must account for the welfare of the individual as well as any impact upon the security of the public body. Suitable relationships should be established between the welfare areas of public bodies – such as human resources and the areas responsible for security – to ensure these areas have a clear understanding around the sharing of information related to employee activities that could increase their susceptibility to cultivation.

References

- Australian Commission for Law Enforcement Integrity, 2013. *Annual Report 2012-13*.
- Australian Crime Commission, 2013. Acting CEO address to the Customs Brokers and Forwarders Council of Australia Incorporated National Conference.
- Australian Crime Commission, 2015. *Organised Crime and Corruption: Risks, Characteristics and Vulnerabilities*.
- Australian Federal Police and Australian Commission for Law Enforcement Integrity, 2014. *Project Apex: A strategic assessment of corruption risk factors in ACT Policing – Project Report to the Integrity Commissioner and the Chief Police Officer of the ACT.*
- Australian Government, 2014. Strategies to mitigate targeted cyber intrusions, Australian Signals Directorate, Cyber Security Operations Centre, Department of Defence Intelligence and Security.
- Centre for the Protection of National Infrastructure (United Kingdom), 2013. *Insider data collection study: Report of main findings.*
- Centre for the Protection of National Infrastructure (United Kingdom), 2013. Personnel Security Risk Assessment.
- Committee on the Office of the Ombudsman and the Police Integrity Commission, 2010. *Report on an inquiry into improper associations in the NSW Police Force. Report No 13/54.*
- Crime and Misconduct Commission (Queensland), 2012. *Anabolic and androgenic steroids: use by police officers.*
- Hart, J., 2010. *Criminal infiltration of financial institutions: A penetration study.* Journal of Money Laundering Control 13(1), pp. 55–65.
- Muravska, J., Hughes, W., & Pyman, M., 2011. *Organised crime, corruption, and the vulnerability of defence and security forces.* Transparency International.
- Office of Police Integrity, 2010. *Discussion paper 2: Sensitive and confidential information in a police environment.*
- People, J., Kirsch, N. and Barnett, P. 2010. *Improper Associations in the NSW Police Force: A review of compliance with policies and guidelines.* New South Wales Police Integrity Commission.
- Rowe, E., Akman, T., Smith, R, & Tomison, A., 2013. *Organised crime and public sector corruption: A crime script analysis of tactical displacement risks.* Australian Institute of Criminology.
- Telstra Corporation Limited, 2014. *Telstra Cyber Security Report 2014: Security insights, trends and impact to Australian organisations.*

ibac independent broad-based anti-corruption commission
Victoria

Level 1, North Tower
459 Collins Street, Melbourne Victoria 3000
GPO Box 24234 Melbourne Victoria 3000
Phone 1300 735 135 | Fax (03) 8635 6444

www.ibac.vic.gov.au