Sensitive and confidential information in a police environment

Discussion paper no.2

Office of Police Integrity
Victoria

About the Discussion paper series

OPI aims to work with Victoria Police to identify policing activities that decrease the risk of organisational and individual susceptibility to corrupt and unethical behaviours and to eliminate the circumstances in which corruption is likely to occur. The Director, Police Integrity understands that successfully reducing the difficulties faced by the majority of honest and honourable Victoria Police officers, as they go about their service to the community, will support the achievement of OPI's objects.

OPI Discussion papers summarise current knowledge and practice about how to prevent the risk of corruption from a specific causal factor. They are guides to corruption and misconduct prevention and to improving the overall professionalism of police. They are not focused on investigations or specific case examples. Discussion papers do not propose to cover all of the technical details about how to implement recommendations. They are written for police of any rank or role, who may then address the specific issue the papers cover in a manner relevant to their own environment or situation.

The Discussion papers are informed by thorough reviews of research findings, literature and reported police practices in Australia and overseas. Even though legislation, laws, cultures and police practices vary from country to country and between states, it has become apparent that police experience common problems. OPI encourages feedback on Discussion papers, and reports of police experiences dealing with a similar issue. Sharing responses experiences and knowledge not considered in these papers could benefit others. This information will be used to update the papers. If you wish to provide feedback and share your experiences, it should be sent via email to opi@opi.vic.gov.au.

Office of Police Integrity

Level 3, South Tower

459 Collins St

Melbourne VIC 3000

Phone 03 8635 6188 **Toll Free** 1800 818 387

Fax 03 8635 6185

Email opi@opi.vic.gov.au

www.opi.vic.gov.au

June 2010

Acknowledgements

OPI would like to acknowledge the assistance of various supervisors within Victoria Police, who gave of their time to share their expertise in the field of information management.

Glossary

CIA	Central Intelligence Agency
LEAP	Law Enforcement Assistance Program
MBTI	Myers-Briggs Type Indicator
NSW	New South Wales
OPI	Office of Police Integrity, Victoria
OIC	Officer in Charge
PSM	Protective Security Manual
SIG	Security Intelligence Group
VPM	Victoria Police Manual
WMI	Weber Motivational Index

Contents

About this document

Police personnel have extensive access to personal and sensitive information, the use of which is protected by government legislation, by guidelines and standards, and usually by an internal Code of Conduct. In Australia, all Australian police organisations with access to national and non-national security classified information are also bound to national standards by the Australian Government Protective Security Manual (PSM).[1] Unauthorised and inappropriate use of information by police officers is a form of misconduct that must result in serious consequences for all officers involved.

This discussion paper arose from extensive research and literature reviews into a number of leak enquiries involving police information. In the process of developing an understanding of the nature of information leaking by police officers, OPI researchers identified a paucity of knowledge within the Australian law enforcement environment.

This paper aims to provide an insight into and generate discussion about the factors influencing leaking behaviour, and to provide options for its prevention, management and treatment. The paper will also use case illustrations from OPI's own investigation files and from the experiences of Victoria Police, to highlight the risks of misconduct and corruption. Whilst specific recommendations are made for Victoria Police, we anticipate that other Australian integrity and law enforcement agencies may find this research useful as they develop their own strategies for addressing this form of misconduct.

The paper commences with a discussion about the dangers inherent in police leaking information, and the potential consequences – for the individual officer, their colleagues, their organisation, and for the community. This discussion states the case that police leaking information should be viewed as a serious form of misconduct and criminal behaviour.

The next section presents the results of research and literature reviews, discussing the individual factors associated with leaking behaviour, including personality, individually held values or beliefs, and motivational factors.

The third section considers the police-operating environment, and those aspects of the work of policing which may contribute to officers' tendency to leak information. In particular, the importance of police culture and accountable leadership are discussed.

---

[1] Australian Government Protective Security Manual, Section A 1.10, Attorney General's Department, 2006

The remainder of the paper discusses processes most police organisations have in place, to address the problem of leaking. Options for strengthening these and considerations of new initiatives will be made.

Introduction

The unauthorised public disclosure of sensitive, officially classified or confidential information by someone with legitimate access to journalistic or media contacts is commonly referred to as 'leaking'. The compromised information is usually referred to as a 'leak'[2].

In Victoria Police, management intervention can be taken against officers who leak and, depending on the nature of the case, officers could be disciplined, criminally charged or dismissed from the organisation.

Serious consequences

Leaking information has the potential to cause harm or place in danger fellow officers, members of the community and other organisations. Leaks of sensitive information, whether intentional or unintentional, can threaten national security[3]. For example, in one Victorian case, confidential information leaked to the media included details of facts provided to police by an informant. Shortly after publication of this information, the informant and his wife were murdered[4]. Other examples in Victoria[5] and in other states[6] indicate a disturbing pattern of longstanding behaviour whereby police routinely leak confidential and sensitive information.

> *The fact of the matter is, some of the worst damage done to our intelligence community has come not from penetration by spies, but from unauthorized leaks by those with access to classified information.*[7]

Such is the extent and apparent intractable nature of this behaviour, the Office of Police Integrity highlighted the unauthorised disclosure of information as a strategic Area of Emphasis in 2010.

Given our current security-conscious environment and increased focus on counter-terrorism, the community could rightly be upset that there are individuals within our law enforcement organisations who deliberately leak information. If that information gets into the hands of criminals, it can help them to plan future attacks or avoid detection. It is well known by law

---

[2] R Borum, R Shumate & M Scalora, 2006

[3] J Bruce, 2003

[4] *Report on the leak of sensitive Victoria Police information,* Office of Police Integrity, 2005

[5] Office of Police Integrity, 2008 & 2010

[6] Criminal Justice Commission, 2000; Independent Commission Against Corruption, 1994; NSW Police Integrity Commission, 2005 & 2008

[7] P Hoekstra, 2005

enforcement agencies that criminals and terrorists pay very close attention to open-source materials such as newspapers and the Internet in order to better understand the strategies and capabilities of an agency. By combining traditional open-source material with leaked classified information, they gain greater insights into the plans, intentions and capabilities of law enforcement organisations. The CIA wrote in 2005:

> *Information obtained from captured detainees has revealed that al-Qaida operatives are extremely security conscious and have altered their practices in response to what they have learned from the press about our capabilities. A growing body of reporting indicates that al-Qaida planners have learned much about our counter-terrorist capabilities from U.S and foreign media.*[8]

To effectively prevent crime and improve public safety, police depend upon reliable intelligence. This enables them to target their activities and efficiently use their resources to achieve the best outcomes for the community.

As the above quote from the CIA suggests, those who wish to compromise the safety of others will use local and foreign media to inform their plans. Because of this, unauthorised leaks of information have the potential to strain relationships with other intelligence and law enforcement organisations. It is impossible for law enforcement organisations, including Victoria Police, to collect all the intelligence necessary to succeed in crime prevention without any support. This is especially the case as the world becomes ever more connected and complicated – particularly due to the Internet. Organisations rely on a global outreach for information to help fill in intelligence gaps. Unauthorised releases of information by police jeopardise other organisations' willingness to share critical information and intelligence.

If a police organisation cannot protect sensitive information, why should they expect other organisations – even those who are collaborators – to be willing to continue to share their information?

The loss of confidence and subsequent ability for collaboration with other law enforcement agencies, whether Australian or foreign, could severely affect Victoria Police's intelligence gathering capabilities in the future.

[8] CIA Memo, June 2002 in P Hoekstra 2005

The psychology of leaking

Individual factors

Psychological research acknowledges that secrecy is a normal part of everyday life, but keeping secrets and concealing information can be an emotional burden.[9] The existence of this burden means that law enforcement organisations and other 'keepers-of-information' need to ensure that their officers are adequately equipped to cope. Therefore, screening, awareness raising and education become important strategies for prevention.

Applying psychological profiling (a strategy already used by many law enforcement organisations for crime prevention) of employees allows an organisation some capacity for behaviour prediction. Identifying an officer's particular traits, preferences and their responses in various scenarios, allows some insight into possible future behaviours. Organisations can use preference identification tools to enhance their workforce's capacity to carry the 'burden' of confidentiality.[10] A summary of some of these tools and how they may be used to predict a propensity for leaking behaviour can be found in Appendix Two. It is important to remember, however, that all personality types are capable of deciding whether to maintain confidential information. At some point, the need to protect what they know for many will come into conflict with other, more basic and more powerful influences than policy or codes of conduct. In 1944, author and political commentator C S Lewis described the powerful influence of what he called the 'inner ring':

> *It would be polite and charitable … to suppose that none of you is yet a scoundrel. On the other hand, by the mere law of averages …it is almost certain that at least two or three of you before you die will have become something very like scoundrels… The choice is still before you: and I hope you will not take my hard words about your possible future characters as a token of disrespect to your present characters. And the prophecy I make is this – to nine out of ten of you the choice which could lead to scoundrelism will come… Obviously bad men, obviously threatening or bribing, will almost certainly not appear. Over a drink or a cup of coffee disguised as a triviality and sandwiched between two jokes, from the lips of a man, or woman, whom you have recently been getting to know rather better and whom you hope to know better still – just at the moment when you are most anxious not to appear crude, or naïf, or a prig - the hint will come. It will be the hint of something which is not quite in accordance*

[9] T Frijns 2005 : A Kelly J Klusas R von Weiss & C Kenny 2001

[10] G Dennis, 2006

> *with the technical rules of fair play: something which the public, would never understand: something which even the outsiders in your own profession are apt to make a fuss about: but something, says your new friend, which "we" – and at the word "we" you try not to blush for mere pleasure – something "we always do". And you will be drawn in, if you are drawn in, not by desire for gain or ease, but simply because at that moment, when the cup was so near your lips, you cannot bear to be thrust back again into the cold outer world. It would be so terrible to see the other man's face – that genial, confidential, delightfully sophisticated face – turn suddenly cold and contemptuous, to know that you had been tried for the inner ring and rejected. And then, if you are drawn in, next week it will be something a little further from the rules, and next year something further still, but all in the jolliest, friendliest spirit. It may end in a crash, a scandal, and penal servitude: it may end in millions, a peerage and giving the prizes at your old school. But you will be a scoundrel."*[11]

Self-awareness, discipline, reinforcement and support are necessary to counter those influences such as those described by Lewis, that may induce leaking. Further discussion and recommendations in this regard will follow.

Intent

Borum et al[12] propose a guide for understanding leaks, based upon a "continuum of intent". Following this reasoning, our next level of analysis is to determine the level of intentionality. Whilst leaks that are unintentional or intentional both cause harm, the strategies for preventing each will differ. Unintentional leaks are made:

- Unknowingly – either the leaker not knowing that the information was protected or that the information has been released;
- Negligently – disclosure occurs as a result of carelessness, or failure to follow correct procedures; and
- Due to impairment – disclosure occurs because of impaired mental or cognitive capacity, often because of intoxication.

If the leak is intentional, a further layer of analysis is required to determine motivation before an appropriate strategy can be determined.

[11] C S Lewis, 1944

[12] Borum et al, 2006

Why do police officers "leak"?

A review of research literature, experiences of other police jurisdictions and observations by Victoria Police representatives provides more insight into the types of officers who intentionally leak and the reasons for police officers leaking information to third parties.

It appears that for some police, leaking information is almost second nature. This leaking may occur for any number of reasons, such as to bring attention to a good news story, to discredit a bad story, or to gauge public reaction to an issue. However, police who leak information for personal reasons, especially those that have access to sensitive information, are of greatest concern. The unauthorised release of information to colleagues, friends and family, neighbours, registered informers and, of course, known criminals also can result in severe and potentially dangerous consequences for police officers and the organisation.

A police officer disclosing information has no way of knowing, nor controlling, how the receiver of that information will go on to use their new knowledge, nor who else they will go on to tell subsequently. A senior member of Victoria Police said a significant risk to information security is a lack of understanding that information 'chunks' can be linked, that people officers speak to may have relationships with other people which, can make their information a dangerous weapon, and that they may be putting their own or other officers' lives at risk by leaking information[13].

A recent review by the New South Wales Police Integrity Commission (2008)[14] found the greatest proportion of alleged leaks were 'accidental' or leaked to others for curiosity or during gossip. Of these, 21 per cent had an obvious benefit for the police officer involved, the majority being for personal satisfaction.

Other motivations for police officers' unauthorised information sharing, identified in literature[15] include:

- ego;
- misunderstanding of their relationship and subsequent 'grooming' or manipulation by the receiver;
- fear – of being bullied, bribed or bluffed;
- financial gain;

[13] Manager, State Intelligence Division, Victoria Police, 26 November 2009

[14] New South Wales Police Integrity Commission, 2008

[15] M Punch, 2000

- lack of awareness of the consequences;
- ideological or political objectives;
- altruism or the belief they are helping a friend;[16] and
- reprisal for real or perceived injustices.

One theory proposed during consultation for this paper was that employees, especially those leaking to media, are disgruntled and want to vent frustration and shed light on issues they feel the organisation has ignored or failed to manage. This hypothesis proposes that when an organisation fails to address the real or perceived concerns of these officers in the manner that the officer believes was adequate, the officer then has little care for policy concerning talking to the media, and feels justified in their actions or is beyond caring about potential consequences.

Although all malicious leaks are intentional, the motivation for all intentional leaks is not necessarily malicious. Further, the degree of intended disruption does not always correspond to the degree of harm that the leak may cause.

Therefore, understanding of the type of goal the leak was intended to accomplish is required to inform appropriate intervention or prevention strategies. For example, when the leaker expects that harm will result from the unauthorised disclosure of information, they often seek to rationalise or justify their behaviour. Intervention in this case focuses upon addressing lies or cover-ups. Where leaking occurred without understanding or predicting the severity of any consequences, an education based approach and assistance to comply is appropriate.

Lessons from research into motivation, beliefs and personality have implications for the psychological assessments made of officers when recruiting into specialist or high-risk areas. Victoria Police currently uses psychological screening to select for psychopathology and various personality traits as part of applicant selection. Psychological assessment of police applicants to specialist units seeks to identify pre-existing psychopathology and to gain an understanding of the applicant's capacity to cope with the demands of the specialist role. This assessment is via a number of opportunities including pre-selection, formal psychological testing, interview, behavioural observation and post-selection 'wellbeing' checks. However, there is no assessment for suitability to hold information confidentially or for capacity to resist vulnerabilities generated either by cognitive and emotional burden or by the operational environment. Assessments that identify

[16] M Argyle, 1988

vulnerability to the above listed motivators enhance the organisation's ability to prevent leaks from the outset.

It has become clear during the course of this review that leaking and its causes are more complicated than just an individual's frustration or ego. Leakers, most likely, do not even think about the reasons why they are about to engage in this behaviour. It is likely that any act of disclosure is overlaid by personality preferences or traits, which, in the absence of any discipline or guidance, can overcome an officer's recognition of their obligations.

Operational environment factors

Our research suggests that leaking behaviour is best understood by focusing not only on the leaker, but also on the situation, intended recipient of the information, and the setting in which the behaviour occurs.[17] These factors make up the operational environment, and typically exert more influence than personality factors alone on the behaviour of officers in possession of sensitive information. Therefore, understanding the operational environment as well as the psychology of leaking is required to develop effective interventions to prevent information leaks.

To manage and prevent misconduct of any type in police organisations, a number of integrated strategies are frequently recommended by practitioners. These include, but are not limited to, education in ethical decision-making, awareness raising, using deterrence and penalties, and improving understanding of existing policies and other documents such as codes of conduct and organisational values.

However, the issue of leaking appears to be mostly symptomatic of a culture that tolerates at best, or condones at worst, breaches of conduct in public office. Therefore, this section of the report seeks to address two major approaches to police culture reform:

- rule tightening; and
- controlling police discretion.

In addition, police cultural reform requires strategies that address informal cultural dynamics such as loyalty, 'codes of silence', and sub-cultures that also contribute to and maintain a poor attitude towards access and use of confidential information.

[17] Borum et al, 2006

Police culture

When it comes to deliberate disclosures of information, police organisations must aspire to a culture where zero tolerance is the accepted norm.

Case study:

After it was established that an officer had leaked information, the officer was suspended from duties with pay. However, this was not the first time this officer had compromised confidential information. Previous disclosures had resulted in verbal reprimands and reminders to follow policy. Despite being aware that the officer had disclosed information inappropriately in the past, there was no review, suspension or other action relating to the officer's security clearances or the continued disregard towards expected behaviour.

The case above suggests a culture where breaches of confidentiality were not taken seriously. Clearly, neither the measures implemented to address the behaviour in the past, nor the ramifications of that behaviour, were effective in altering the pattern of this officer's conduct. It is possible that the previous leniency shown to this officer contributed to his or her decision to continue to reveal information.

Supervision and accountability

All police organisations have an attribute shared by few other organisations – the ability to use discretion is actually greater the lower one sits in the hierarchy. This discretion is exceptionally difficult to oversee, as the nature of routine policing gives it low visibility, both to management and to other regulatory mechanisms. Much of what police officers do is invisible to their senior officers and also goes unrecorded. Such invisibility permits the officers the freedom to interpret their role and provides for high autonomy but low accountability.

Operational autonomy can allow basic assumptions and beliefs constructed by officers to flourish unchallenged. These taken-for-granted assumptions become the true determinants of the organisation's culture. They are the source of unspoken guidance for "how we do things around here" and often inform practised methods and norms. [18]

[18] Ted Bellingham, National Police Training, Bramshill, UK

Case study:

Responsibility for police officer leaking must not fall on them alone; line managers are also responsible for any failure to conduct their duty properly. They are there to supervise. A senior member of Victoria Police with knowledge of one case said:

There was not enough supervision. The supervisor was one of them not so long ago, and was brought up through the same culture. Stronger leadership is required[19]

We acknowledge that officers have a large amount of autonomy, responsibility and scope to perform their duties. Given these necessary risks, it is irresponsible for guidance and support to be lacking in any way. Daniel Carlson, Associate Director of the Institute for Law Enforcement Administration wrote:

> *Individuals who provide guidance and direction from the top of the organisation have a powerful impact on the manner in which the agency will perform, because they are the ones who form and articulate the overall vision for the department. So when they equivocate or, worse still, remain silent on issues buffeting law enforcement, this behaviour amounts to a virtual abdication of leadership responsibility*[20]

A culture of permissive supervision can create the space for leaking to occur. By effectively supervising and oversighting environments with high operational autonomy, supervisors can positively influence the prevailing culture. Some specific suggestions for achieving this are listed in Appendix One.

According to Schein (1992), the most powerful primary mechanisms through which leaders of organisations typically reinforce their desired organisational culture, in order of importance, are:

- What leaders pay attention to, control and measure
- Leaders' reactions to critical incidents and organisational crises
- Deliberate role modelling, teaching and coaching by leaders
- Criteria for the allocation of rewards and status
- Criteria for recruitment, selection, promotion, retirement and dismissal[21].

[19] Manager, State Intelligence Division, Victoria Police, 26 November 2009

[20] Daniel Carlson, pg 84, 2005

[21] Schein, 1992

Other strategies such as organisational structure, procedures, and formal statements of organisational values or missions are secondary or less influential mechanisms.[22] These secondary strategies influence culture only if they are consistent with and support the primary mechanisms listed above. Police organisations traditionally devote a disproportionate amount of energy to these secondary mechanisms to the detriment of the primary strategies shown to have an effective and sustained impact upon culture.

[22] Schein, 1992

Education and awareness raising

Many police organisations have an information security strategy that already includes providing officers with a code of conduct, regularly updated policies and training courses. However, the absence of repeated, regular, frequent, and clear promotion of the expected behaviour and practice appears to be a common criticism. A NSW Police Integrity Commission study[23] into unauthorised disclosure of confidential information to the media found that a key deterrent strategy was ensuring police were aware of the consequences of leaking information, that the consequences were clearly understood, not just hinted at, and that there was a belief that action *would* be taken.

A Victoria Police representative advised that a limited amount of information is provided during the training of police recruits regarding the access and disclosure of confidential information. Information Technology presenters cover the topic in the context of using the Law Enforcement Assistance Program (LEAP). However, it is not discussed during Law presentations or as part of their newly introduced ethical practice modules.[24]

No specific training or information is delivered to officers about dealing with confidential information throughout their career. Information is available on the intranet, and officers are encouraged to contact the Human Source Management Unit for advice or assistance as required[25]. However, this approach relies on officers recognising that they are going to be dealing with sensitive information and understanding the risks inherent *before* any interaction occurs. Capacity limitations of the Human Source Management Unit mean that organisation-wide delivery of training is not possible. Consultations have commenced with the Victoria Police's Education Department to negotiate delivery of training on this topic.

Any education strategy must cover more than policy details. The consequences of officer naïveté and the vulnerability of officers as targets for information-seekers should be included in training. Police officers need to understand that they too possess the same susceptibilities as all humans. There are many examples of police officers gradual exposure to corrupt behaviours or improper ideologies and building up of a tolerance or

[23] NSW Police Integrity Commission, 2008

[24] Instructor, Education Department, Victoria Police, 18 December 2009

[25] The Human Source Management Unit of Victoria Police is recognised as an internal resource, due to their expertise in the management of sensitive information.

sympathy for such activities that eventually develops into active corruption on the officers' part[26].

Police officers, by virtue of their role, are exposed to community contacts that may have alternative political views, be of questionable character or have their own agendas in liaising with police. Given community contacts may also have links to other individuals and other organisations, it is impossible to overstate how important it is that police officers are aware that a community contact may use an officer as an intelligence source for his or her own means.

> *Why won't people protect themselves? ….the media target us…members are vulnerable when they are not aware of this.*[27]

Victoria Police human source practitioners[28] identified a training regime conducted by the Royal Canadian Mounted Police as representing best practice in education on this topic. Four tiers of training exist, covering policy and basic skills through to high-risk management. Students for the progressive levels of training are selected according to local workplace needs or specialist requirements. The initial package is online and must be completed before officers are involved as human source managers. Further training packages involve group attendance where a range of issues are discussed including ethics, risk, practical skills and legislative requirements. These courses utilise experienced practitioners and involve a minimum five days of face-to-face instruction. As they progress through the tiers, the students are introduced to more challenging practical exercises. To achieve a consistent skill level across Victoria Police, it is proposed that all specialist investigators and officers dealing regularly with information sources complete the first two training tiers as a minimum.

To complement the training syllabus, the Victoria Police State Intelligence Division also provides specialist support to work areas through tailored presentations. These presentations were reported to be particularly effective for refreshing knowledge and addressing member concerns, as well as ensuring the overall training syllabus remains relevant[29]. A formal evaluation of this training to confirm these claims was not available and should be conducted.

There is room for further improvement in information management education within Victoria Police. Primarily this should occur through reinforcement that

---

[26] *Ethics in Policing*, First National Conference of the Australian Police Ethics Network Conference paper 1999

[27] Manager, State Intelligence Division, Victoria Police, 26 November 2009

[28] Manager, State Intelligence Division, Victoria Police, 11 February 2010

[29] ibid

confidentiality of information and intelligence is a means to achieve timely, cost effective and successful investigation outcomes. The recent introduction of a new training tier, and plans to expand tailored presentations to newer officers, recognise and begin to address the level of risk involved in the management of confidential intelligence. Expanding the training environment enables all officers to recognise opportunities for identifying potential human sources and their information, identifying the associated risks and managing the interaction with confidence and integrity.

Policy documents and availability of written guidance

Code of Conduct

A small section of the Victoria Police Code of Conduct discusses confidential information. It is very clear in this Code that access to and disclosure of information is forbidden, other than that legitimately required when undertaking a duty.

However, the Code makes a general reference to 'good practice', without definition, and suggests that such behaviour *'may'* (author emphasis) be unlawful. Including examples of what constitutes a leak of confidential information can enhance the Code.

As stated earlier, the most frequent leaks of information are accidental[30] and/or secure no benefit for the officer. The wording of the Code may give the understanding that the only dangerous leaks are those to criminals. Emphasising that providing *any* information without authorisation is a leak, regardless of to whom it was given and whether or not benefits were expected, improves this Code.

Intranet

The organisation's intranet is often an employee's first point of call when looking for information and guidance on responsibilities, policies or issues that affect them. For the purposes of this research, we identified no less than eight separate policies on the Victoria Police network that had reference to the management, access or release of information. Each policy cross-referenced up to 13 other policies, manuals or Acts of Parliament. It must be difficult to search for guidance when dealing with confidential information if you are an officer of Victoria Police. It was not surprising to hear from senior Victoria Police personnel that they felt frustration at their officers' apparent lack of awareness or understanding of policy, and, in some cases, lack of knowledge that guidance existed at all.

[30] NSW Police Integrity Commission 2008

The Victoria Police intranet also contained out-of-date information, 'dead' links and pages promising up-to-date information that were blank. For example, the Intelligence and Covert Support Department's Guidelines and Processes web page has remained blank since it was last updated in June 2006.[31]

Policies

When asked about possible systemic factors contributing to the risk that officers will disclose information, a senior Victoria Police supervisor mentioned the current policy that deals with the management of human sources. He stated that it was too long and "unreadable". Combined with the knowledge that managers are unlikely to hold officers to the policy requirements (see Supervision and Accountability), he believed officers would be tempted to operate outside of formal policy and procedure. The supervisor stated that he was aware of many instances where officers have failed to register contact with a source or communication with a community member to avoid "troublesome paperwork". This means that appropriate risk mitigation cannot occur. The supervisor said:

> *Members only read the policy when they are in trouble, then try to fit their behaviour to be in line with policy.*[32]

Leaks of information can be prevented by minimising misinterpretation of policies, increasing awareness of policies and procedures, and making it easier for officers to do the right thing. Simplifying guidance by combining all relevant codes, guidelines, policies and standards relating to confidential information into a single, one-page overview document would assist officers. This can be achieved via the intranet and the use of web page linkages that take the reader to the specific area of information management of interest.

Awareness of vulnerability is no more effective by itself than any policy that is only visited by officers when they are in trouble. Effective processes and support for officers to implement the policies must exist.

Documentation and recording of information

Conducting a risk assessment of potential hazards to the officer and to the organisation prior to any meeting planned with new community contacts for the purposes of exchanging information is highly recommended. Prior to any future planned meetings, officers should refer to these assessments and update them with relevant information. For unexpected contacts, recording

---

[31] Accessed 30/09/09, http://intranet/content.asp?Document_ID=6664

[32] Manager, Surveillance Services Division, Victoria Police, 5 November 2009

the details of the conversation and exchange of information as soon as possible, and conducting a risk assessment, allow risks to be identified, the appropriate supervisor to be notified and a management plan to be developed.

Police have varying levels of access to confidential information. Police officers who work in intelligence units are exposed to greater information security risks due to the nature of the information they hold and to their increased discretion and autonomy.

> *Workplaces that receive, create and/or disseminate documents containing national security information must comply with the Australian Government Protective Security Manual (PSM).*[33]

It is good practice to implement an audit program of all units and departments that deal with highly sensitive information to assess their level of compliance with the relevant PSM standards and identify areas where mitigation or management strategies are required.

Expected behaviours

Victoria Police policies are clear and unambiguous in terms of what must occur before releasing information to the media. In addition, the Victoria Police Code of Conduct clearly forbids personnel from making public comment. However, there is not a ready definition of "making public comment". The Code of Conduct does not contain any examples, scenarios or references to the *Police Regulation Act* 1958 regarding public comment. There is a lack of instruction on discussing work matters outside of work where there is not an actual media engagement strategy. Discussions and releases of information through gossip, accidental disclosure and curiosity are not covered and is it likely that many officers are committing breaches of their duty regularly when discussing work in social circumstances and are making comments that, if overheard or recorded, could be quite damaging, embarrassing or controversial.

[33] Victoria Police Manual 111-8.1

Case Study:

The following email was accidentally sent by a police officer to the person termed a 'squeezer' instead of the intended recipient – a friend who parks at a McDonalds restaurant.[34]

From:
Sent: Thursday, 25 February 2010 12:36 PM
Subject: RE:
Hey,
Whats this crap about? (this) fella is the one that has grounds of Mental Impairment. What a squeezer...
Craig.
PS
Stop parking at Mc Donalds!! ....your taking up the parking space of some Fat, smelly lower class F wit from Frankston north who needs to survive on 20,000 calories a day to maintain their disability support payments from Centre link ...So STOP IT.

The content of the email raises concerns about the officer's attitude towards people with a mental illness and towards the community of Frankston North, which are important issues when considering the professionalism of this officer. However, this case also highlights the embarrassing consequences for the reputation of this officer and the impact such behaviour has upon the organisation and its standing in the community. The behaviour is also an illustration of uncontrolled use of police information technology to share personal opinions.

Strengthening and expanding guidance to include instruction regarding making public comment to friends and/or family could also assist in the prevention of unintentional leaking. Whilst it is implied, some small amendments to the wording of the Code of Conduct will make this expectation clearer and stronger.

> *Most releases of information are from people who legitimately had access to the information…they just forget their role. Often members forget they are in public office. What they have access to is actually owned by the State of Victoria. It is not theirs to discuss* [35]

Where email or other IT systems are involved, infrastructure which compels the sender to assess and identify a security classification for the contained information prior to it being successfully sent ensures the officer has had to consider the consequences of inappropriate or inadvertent release of the information, and has decided upon a course of action.

---

[34] "Fat and smelly" Frankston jibe lands cop in hot water. Herald Sun, Melbourne, 6 April 2010

[35] Manager, State Intelligence Division, Victoria Police, 26 November 2009

Continuous reminders

Currently, it appears officers ignore protocols and guidelines because they are considered cumbersome. Officers lack understanding of the importance of protocols and guidelines and why they were implemented in the first place.

Communication and education must be relevant and ongoing. One-off sessions implemented in reaction to crises or breaches do not contribute to sustained cultural change. Officers need to receive education and be reminded of responsibilities and inherent risks at critical career points. Officers change roles, change levels of rank or responsibility, move to different jobs, or a change occurs in their relationships. Each of these experiences can potentially change the level of an officer's security clearance and their exposure to confidential information. It is therefore an opportune time to review and reflect on their behaviour, their associations and to reinforce their obligations.

It is recommended that a communication and education strategy is implemented that includes:

- promoting employee responsibility when discussing police matters in public domains;
- increasing understanding of what constitutes 'misconduct in public office';
- increasing understanding about why the policies and processes are there and their context; and
- managing relationships with media appropriately.

Breaches of discipline

Although some leaks of information may be accidental or occur due to a lack of awareness or knowledge, as discussed earlier there will be some instances where information is deliberately leaked.

The Office of Police Integrity wrote in 2005:

> *Even with increased training in informer management, these strengthened policies and procedures [as recommended in the OPI's report] will not prevent the disclosure of all sensitive information if a member decides to ignore the restraints that legislation, policy and procedures impose and embarks on a course of conduct contrary to those restraints.*[36]

It is difficult to prevent the misconduct of officers who deliberately undertake to leak information despite their awareness of policy, receipt of education, or guidance to protect their vulnerability. Some are deterred if the consequences for this misconduct have been made clear, promoted widely and are well understood.[37] Officers also need to believe that their behaviour *will* be detected and that action *will* be taken. Emphasising the penalties that apply and providing public case examples of officers who have been disciplined or dismissed for such behaviour has effectively deterred police officers from considering this form of misconduct. Tightening the language used in policies and codes of conduct from 'may' to 'will' also helps to achieve this stronger message.

However, it is the opinion of some police that leaks occur so frequently that it is too difficult to identify who leaked the information, to investigate it thoroughly and obtain an outcome. Some Victoria Police officers stated that they do not have the resources to investigate these cases, each perhaps taking months, when there is no way to narrow down the list of people who had access to the information.

In our current environment, information is readily shared and more people have access to more information than ever before, e.g. internet, mobile phones, Twitter and Facebook. Whilst investigating leaks is much more difficult, police organisations should be wary of promoting a cultural norm of acceptance or of suggesting that it is all too hard.

Instilling a need-to-know culture, in order that the least number of employees have all of the information about sensitive or confidential issues, goes some

---

[36] Office of Police Integrity, 2005, p30

[37] Pogarsky and Piquero, 2004

way towards preventing inappropriate information sharing. Creating this need-to-know culture in a positive manner can be achieved by reinforcing the principles through messages that emphasise that:

- it is not that the organisation does not trust employees – it is because information-seekers can use practices that can trip up even the most experienced employee; or
- if an officer does not know, the officer cannot tell.

Initiatives such as this have proven useful in other organisations that sought to build a culture where information is protected and where employees understand this principle and are committed to this goal.

Conclusion

The nature of policing means that police officers will, through necessity, regularly encounter personal or confidential information and use that information to conduct legitimate police business. They are also responsible for the security of that information. The nature of policing means that officers are in regular contact with those in society who would seek to utilise that information for their own purposes and/or criminal enterprise.

Unauthorised disclosure of information is a leak, and, if intentional, will be treated as misconduct in public office. Police organisations seeking to prevent or reduce the risk of officers behaving this way need strategies on a number of levels, and should not rely on policies or codes of conduct alone.

Police organisations can strengthen their recruiting and promotion assessments to identify those officers either unsuitable or at risk for engaging in this behaviour. A culture of zero tolerance is encouraged, with appropriate sanctions promoted and consequences carried out. Supervisors should take a greater interest in their officers' associates, and ensure that leaking is not considered acceptable practice. Efforts to reduce operational autonomy without compromising effective policing should be demonstrated by police supervisors. Education about the organisation's policies, standards and expected behaviours should be included in all formal training opportunities, and repeated at critical career points throughout an officer's career. Policies should be clear and easily understood, should provide examples, and should be easy to comply with from a procedural perspective. Where an officer has breached the standards expected, decisive action is required and the taking of such action should be made known throughout the organisation. This forms part of the education strategy. Finally, developing an acceptance and understanding of the principles underpinning a need-to-know culture assists in helping officers to reduce their own risk of being the target of information seekers.

Appendix One – Reducing operational autonomy

Operational autonomy occurs within the policing environment where high levels of discretion exist in the absence of close supervision, monitoring and/or guidance. The following suggestions can counter the risks posed by operating with high levels of discretion:

- Police officers brief the OIC of their unit, via a written and verbal report prior to engaging with a community contact and provide a written and verbal debrief following the contact that justifies the reasons for the contact, and covers matters discussed and information obtained, post interview.
- The OIC assesses an officer's conduct and activity for unusual amounts of contact and for properly recorded and reported activity, and reviews contact reports for any officers of note.
- The policy on liaising with media is communicated, with an emphasis on *no contact whatsoever with media personnel* highly recommended.
- Barriers to management intervention are removed. Some examples include taping of community contact conversations, vehicle tracking systems and incident mapping systems.
- No single officer has exclusive access to a community contact. Whilst this may be damaging for rapport it may also assist the officer to avoid becoming overly familiar with a particular contact. It also protects the officer from vexatious allegations about their own conduct.
- Officers working in sensitive environments should be assessed quarterly to ensure any issues influencing their ability to carry out their role are identified early and actively managed, and the officer is provided appropriate support.

Appendix Two – Using psychological profiling to predict leaking behaviour

The following summary describes how different personality types may generally approach the requirement to maintain confidential information.[38]

The Myers-Briggs Type Indicator (MBTI)[39]

Description

Personality preferences in the MBTI are presented as four domains, each understood as a continuum between two polar opposites. The more strongly an individual scores in their preference type, the more likely it is that the preference will exert influence over their behaviour – whether they recognise it or not. The four continuum dyads are:

- Introvert (I) vs Extrovert (E), describing how an individual mentally recharges themselves;
- Sensing (S) vs Intuitive (N), describing an individual's preference for taking in information;
- Thinking (T) vs Feeling (F) describing their preference for decision-making style; and
- Judging (J) vs Perceiving (P) showing how and individual prefers to organise their daily life.

Each individual's type is determined by his or her place along each continuum.

Application

The I – E and S – N dyads have most relevance to predicting how an individual may view confidential information:

Extroverts (E) value interaction. They tend to view communication as vital and more valuable than Introverts do. This has both positive and negative implications. E-types tend to receive more information and more easily than I's. They also give out more information in the course of their day. Because of the large volume of information coming in and out for E's, they need to pay more attention to their sources, the recipients and the details of the information. If E-types are responsible for sensitive or confidential

[38] Source: G Dennis 2006

[39] Myers, Isabel Briggs; McCaulley Mary H.; Quenk, Naomi L.; Hammer, Allen L. 1998

information, they will need to use even more energy and vigilance to manage the need-to-know aspects of their communication. If their energy is low, additional caution is required, as the preference for all individuals is to behave instinctively from comfortable habits. They will need to choose to behave in an opposite manner to that which comes naturally.

Introverts (I) will find it easier to hold confidential information because they tend to be more selective about their disclosures and instinctively less communicative. However, while they can be expected to be good at keeping secrets, I-types may be vulnerable to those very few in which they do confide. I-types also often give away clues via body language when they are withholding, calculating or otherwise thinking about strategic information.

Extroverts who are also Sensing (S-types) often feel a need for specific detail in both giving and receiving information. Without self-awareness of this, they can be more susceptible to disclosure. Introverts who are also S-types are similarly vulnerable, once they have decided to disclose.

Intuitive (N) types feel a need to provide the big picture to others and prefer to receive the broad perspective on issues. This may lead to the possibility of disclosing general information even while withholding specifics.

Recommendation

This test is broadly available and does not need to be administered by a psychologist. It is available online and can be self-administered. It may provide additional assessment capability for all police personnel as an adjunct to other selection tools. It also has potential for the selection and education of police officers entering roles where information management is a core function of their duties, e.g. detectives, intelligence, information technology, source handling, counter terrorism, managers and high-risk units. The test should not be used to exclude selection; rather the results should be used to educate and create self-awareness so that the officer can take measures to address any identified risks.

FIRO-B Test[40]

Description

This test measures several dimensions of social need.

Application

Those individuals scoring with a high need for social connection with others, close affiliations and emotional warmth are less likely to see or experience the need for secrecy, as a preference. Without support and self-awareness, these individuals are less likely to succeed in maintaining confidential information against any pressure to disclose. They are also likely to experience conflict between competing personality needs. For example, in positions where the information is required for decisions with large implications, control over the information is required. For individuals with a need to collaborate in order to come to their decision, deliberate focus on tactics to assist them to maintain confidentiality is required if they wish to avoid disclosure.

The test is also broadly available, can be taken online, and does not require a psychologist for interpretation of the results.

Recommendation

This assessment may be useful to assist the selection of officers to highly sensitive environments and high-risk areas. It may also be used more generally to select employees into management positions within a police organisation.

[40] W C Schutz, 1958

Weber Motivational Index (WMI)[41]

Description

The WMI is designed to assess the kinds of needs and values that people see as important considerations in making decisions about their work. It is based on Abraham Maslow's "Needs Hierarchy" concept of human motivations.

Application

This framework identifies and ranks 14 motivational drivers, and can be used to determine an individual's position regarding the need to maintain confidentiality. For example, an individual found to place a high priority on acceptance and on risk avoidance will approach secrecy and the issues of disclosure very differently from someone who values recognition, being successful, enterprising and a risk taker.

Recommendation

It is recommended as a remote profiling tool, e.g. an interview framework for reference checking prior to a selection decision.

[41] M Weber 2004

Resources

Australian Securities & Investments Commission (2009), *Handling confidential information: best practice guidelines*

Criminal Justice Commission (CJC) 2000, *Protecting confidential information: a report on the improper access to, and release of, confidential information from the computer systems by members of the Queensland Police Service*, CJC, Brisbane.

Crime and Misconduct Commission (CMC) Queensland (2005), Information security: Keeping sensitive information confidential, Building Capacity Series No.7, February 2005

National Policing Improvement Agency (2010), *Guidance on the Management of Police Information* 2nd Edition

References

Argyle M (2000) *The psychology of interpersonal behaviour*, 4th Edition, Penguin Press, New York

Attorney General's Department (2006) *Australian Government Protective Security Manual, A1.10 – A1.22*, Australian Federal Government, ACT

Australian Police Ethics Network (1999) Ethics in Policing: First national Conference of the Australian Police Ethics Network, Conference paper

Bellingham T (2000) Police culture and the need for change, *The Police Journal*, January 2000, 31-41

Borum R, Shumate R S & Scalora M (2006) Psychology of "leaking" sensitive information: implications for Homeland Security, *The Homeland Security Review: A Journal of the Institute for Law and Public Policy*, 1 (2), 97-111

Bruce J (2003) Laws and leaks of classified intelligence: The consequences of permissive neglect, *Studies in Intelligence*, 47, 39-49

Carlson D P (2005) *When cultures clash: Strategies for strengthening police-community relations*, 2nd Edition, Pearson Education, New Jersey

Criminal Justice Commission (2000) *Protecting confidential information*, Brisbane

Dennis G (2006) *Spying, security and the psychology of secrets*. http://ezinearticles.com/?Spying,-Security-and-the-Psychology-of-Secrets&id=32627, accessed 22/12/2009

Frijns T (2004) *Keeping secrets: quantity, quality and consequences*, Academic Thesis submitted 22 February 2005, Department of Social Psychology, Free University, Amsterdam

Herald Sun (2010) "Fat and smelly" Frankston jibe lands cop in hot water, *Herald Sun*, Melbourne, 6 April

Hoekstra P (2005) *Secrets and leaks: the costs and consequences for national security*, Heritage Lectures # 897, The Heritage Foundation

Independent Commission Against Corruption (1994) *Report on investigation into matters relating to police and confidential information*, Sydney

Kelly A, Klusas J, von Weiss R & Kenny C (2001) What is it about revealing secrets that is beneficial? *Personality and Social Psychology Bulletin*, 27, 651-665

Lewis C S (1944) *The Inner Ring* Memorial Lecture at King's College, University of London, http://fairuse.100webcustomers.com/eg/cs-lewis.html, accessed 24/12/2009

Myers, Isabel Briggs; McCaulley Mary H.; Quenk, Naomi L.; Hammer, Allen L. (1998). *MBTI Manual (A guide to the development and use of the Myers Briggs type indicator)*. Consulting Psychologists Press, 3rd Edition

New South Wales Police Integrity Commission (2005) *Operation Cobalt*, Sydney

New South Wales Police Integrity Commission (2008) *Unauthorised disclosure of confidential information by NSW police officers*, Sydney

Office of Police Integrity (2005) *Associations that compromise Victoria Police – risks and remedies*, Melbourne

Office of Police Integrity (2005) *Report on the leak of sensitive Victoria Police information*, Melbourne

Office of Police Integrity (2005) *Investigation into the publication of "One Down, One Missing"*, Melbourne

Office of Police Integrity (2007) *Annual Report 2006-2007*, Melbourne

Office of Police Integrity (2008) *Exposing corruption within senior levels of Victoria Police*, Melbourne

Office of Police Integrity (2009) *Annual Report – financial year ending 30 June 2009*, Melbourne

Office of Police Integrity (2010) *Information security and the Victoria Police State Surveillance Unit,* Melbourne

Pogarsky G & Piquero A R (2004) Studying the reach of deterrence: Can deterrence theory help explain police misconduct? *Journal of Criminal Justice*, 32, 371 -386

Punch M (2000) Police corruption and its prevention, *European Journal on Criminal Policy and Research*, 8, 301-324

Schein, E (1992) *Organizational culture and leadership*, San Francisco: Jossey-Bass

Schutz, W.C. (1958). *FIRO: A Three Dimensional Theory of Interpersonal Behavior*. New York, NY: Holt, Rinehart, & Winston

Victoria Police Code of Conduct

Victoria Police, *Intelligence and Covert Support Department Guidelines and Processes,* http://intranet/content.asp?Document_ID=6664, accessed 30/09/09

Victoria Police Manual, Version December 2009

Weber M (2004) Profiling for leadership analysis, *Applied Behavioural Sciences*, 7 (4), 6-12