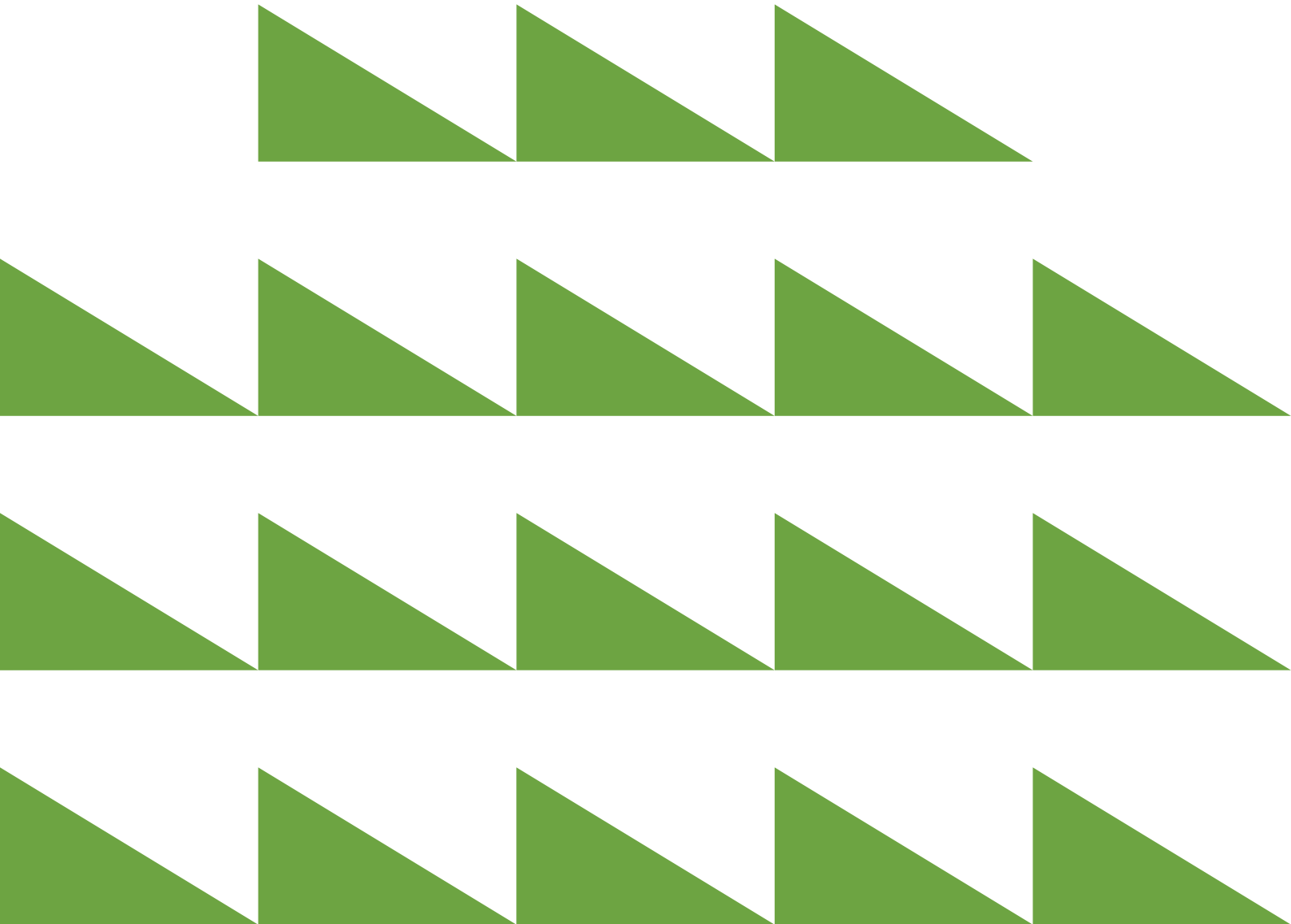
ibac independent broad-based anti-corruption commission
Victoria

Unauthorised access and disclosure of information held by Victoria Police

An analysis of corruption risks and prevention opportunities

September 2019



Contents

In 2017, a private investigator, who was also a former Victoria Police employee, was expected to be charged after seeking official police information from previous colleagues. This former police officer established a company with another former police officer, which specialised in investigating compensation fraud for major insurers and WorkCover.[39] With many ex-police officers having transferable skills to the private investigations and security industries, and reports of former police establishing related businesses, there is an ongoing risk of Victoria Police employees being targeted for information by former colleagues.

3.2 Risks at the organisational level

This section focuses on the common corruption risks IBAC has identified as associated with Victoria Police systems and processes for information security related to employees accessing and disclosing information without permission. This type of corrupt behaviour is often enabled by gaps or deficiencies in policies, systems and procedures.

3.2.1 Lack of detection of unauthorised access and disclosure

Victoria Police has had longstanding external scrutiny (currently by OVIC) of its information management arrangements, and this has led to an established risk management process. With the introduction of the VPDSF across the public sector, Victoria Police is sharing its experiences to assist other public sector entities to apply information management frameworks that better incorporate security and training.

Victoria Police has made few proactive detections of unauthorised disclosure of information, including to the media, political groups and other entities. Disclosure investigations can be resource-intensive and face challenges related to journalists being protected from revealing their sources as outlined in section 3.1.2. High-profile and sensitive matters are usually those which have a greater impact on the community due to the seriousness of offending, the level of harm the alleged offences have caused, or due to the role the people involved have in the community.

Noting that unauthorised disclosures of information may follow unauthorised access to police information systems, Victoria Police is advised to consider shifting its emphasis to consistent detection of the unauthorised access of information in sensitive and high-profile cases. This could include an ongoing audit program of information in these cases, which may also detect unauthorised disclosures, including those to organised crime figures.

Another risk for unauthorised access and disclosure of information is that there may be lower levels of information security practised by an employee after an employee submits their resignation but is still employed by Victoria Police. This is due to a perception by employees that there is both reduced detection and reduced consequences of information misuse during this time since they are soon to leave the organisation. Victoria Police advises IBAC it is introducing targeted auditing to address this risk.

To address these risks of unauthorised access and disclosure of information, IBAC recommends that the resourcing of Victoria Police's information management security systems be further strengthened, including through an extensive proactive program of audits. Strengthening these systems would also assist Victoria Police's ability to detect unauthorised access and disclosure of information by its employees.

3.2.2 Education and training

Victoria Police has around 21,000 full-time equivalent employees with approximately 3960 of these being Victorian public service (VPS) employees, including police custody service officers, forensic officers and VPS grade employees.[40] A large number of VPS employees are lower level employees (VPS 2 and 3) in support roles, and often have the same access as police to law enforcement data and official information, including intelligence.

Victoria Police employees receive training on information management, including information security and appropriate use as part of their induction, either as recruits at the academy or via an induction program for non-police employees. Training is also delivered annually via an online learning module and in courses delivered for officers when they are promoted. However, the majority of Victoria Police employees stay at the same rank or at VPS level for a significant part of their career, meaning information management training is only delivered via online modules, or as part of other training. This means higher ranked employees are well trained in information management and employee obligations, but many lower level employees (who may access the data more often) are likely to have received formal training only once, at the beginning of their careers, and therefore have a lower understanding of the risks.

A 2015 report from the former Commission for Privacy and Data Protection stated Victoria Police employees recognise data security is a critical aspect of their jobs; however, they may still not be aware or mindful of the full range of risks. The report also found Victoria Police employees generally had the intent to comply with information security but the systems and resources of the organisation needed to improve the level of technical, preventative and educative support for employees.[41]

[40] Victoria Police, *Employees by Location at June 2019*, July 2019..

[41] Commissioner for Privacy and Data Protection, *CPDP – Victoria Police: Wave 1& 2 – results (abridged)*, March 2015.

4 Drivers of corruption risks related to information access and disclosure

4.1 Personal issues of employees

The personal issues and circumstances of employees has been identified by both IBAC and integrity partner agencies as a key driver of intentional misuse of official information. Personal issues identified in IBAC investigations often relate to the overall health and wellbeing of the person alleged to have committed police misconduct or corruption, and this is often negatively impacted by alcohol and illicit drugs, breakdowns in personal relationships, gambling or periods of poor mental health.

Victoria Police has a range of employee assistance programs in place that assist with mitigating the risks of unauthorised access and disclosure of information driven by personal issues. It also has a Mental Health Strategy and Wellbeing Action Plan to strengthen these programs and encourage more people to seek help when needed. The plan notes how the stigma associated with mental health has previously dissuaded people from asking for help.

In 2016, Victoria Police published the *Victoria Police Mental Health Review*, an independent review into the mental health and wellbeing of Victoria Police employees.[42] The review found that more people are using support services due to more services being offered and more help being accepted. This followed the 2015 Victorian Equal Opportunity and Human Rights Commission (VEOHRC) review to examine sex discrimination and sexual harassment in Victoria Police. While services set up in response to this are focused on sex discrimination and harassment, the traditional support services are available to address other personal issues. It is expected these programs and initiatives will lead to a decrease in information misuse driven by personal issues of employees.

[42] Victoria Police, *Victoria Police Mental Health Review 2016*. Published May 2016.

CASE STUDY 7 – IBAC INVESTIGATION UNCOVERING LEAP USE FOR PERSONAL INTEREST

In early 2017, IBAC commenced an investigation into allegations that a Detective Leading Senior Constable was attending a metropolitan strip club and associating with the manager who was believed to be affiliated with an outlaw motorcycle gang.

The investigation sought to determine whether the officer had inappropriate relationships associated with the strip club, any criminal involvement or whether they were potentially compromised.

IBAC found that the officer had an ongoing association to the strip club dating back to at least 2011, and received favourable treatment in the form of free entry and free alcoholic drinks. This favourable treatment was not isolated to the officer, with the strip club having a business practice of giving free entry to Victoria Police employees (and other occupations or groups of people) and supplying them with complimentary drinks.

The investigation found the officer had substantial debts, including the balance of their 17-year-old mortgage being two and half times the amount the officer had purchased the residence for, and nearly $80,000 in credit card debt. This type of financial position puts a police employee at risk of compromise. The investigation also found the officer had withdrawn more than half their salary in cash near the strip club. The officer was frequently drinking alcohol to excess and admitted to IBAC they drove after consuming alcohol at the strip club.

On numerous occasions, the officer accessed LEAP for police information about their associates, some of whom they met at adult entertainment venues or through the sex work industry. On at least one occasion, the officer accessed and then disclosed police information to an employee of the strip club. On another occasion, the officer accessed and used police information for the apparent purpose of gaining the personal details of a sex worker who the officer had hired and lent money to.

The officer resigned from Victoria Police in early 2018 while under investigation. The officer subsequently also pleaded guilty to charges relating to the unauthorised access, use and disclosure of police information.

4.2 Social media use

Social media users, including police employees, may upload large amounts of personal information and opinions to both public and restricted social media platforms. Victoria Police recognises the risks social media use presents to its employees and the organisation and has a longstanding social media policy. However, it continues to face conduct issues related to social media, including the use of social media platforms to discuss work activity.

IBAC has identified that police employees – from recruits, to senior command, to ex-employees – regularly use Facebook and other messaging platforms to contact colleagues and discuss work activities. In cases where these messages may be password protected, Victoria Police employees may not appreciate the information they upload to these platforms as a risk or that the social media platform may now 'own' the information. This is likely to also increase the risk of official information being leaked by employees via social media and encrypted platforms without detection.

It is often difficult for law enforcement agencies to detect misuse of social media. This can be due to resourcing, privacy restrictions on social media accounts and difficulties in obtaining information via warrants when social media hosts are located internationally. Due to these difficulties, IBAC assesses that information disclosure on social media is often not detected and therefore under-reported.

To combat this, Victoria Police policy allows social media checks to be conducted upon potential recruits and employees; however, it does not proactively monitor social media to identify inappropriate information disclosures by its employees.

4.3 Information sharing with approved third parties

Victoria Police information is frequently shared with approved third parties. These include other law enforcement agencies across Australia and sometimes overseas, other Victorian public sector agencies and the federal government.

Under the VPDSF, agencies must have a level of assurance that approved third parties will offer the same, or better, protection of that information.[43] Since the roll-out of the VPDSF, and the majority of public sector agencies having been required to adhere to the standards since June 2016, it is likely that secure information sharing practices across the Victorian public sector will have improved over the past few years. However, intelligence suggests that due to limited detection and auditing by Victoria Police, unauthorised information access and disclosure of Victoria Police data by third parties remains an issue for the organisation.

The ways in which these third parties use and store data that is accessed and received also affects the risk of Victoria Police information being misused. While the risks of third-party employees misusing information are similar to employees of Victoria Police, these risks are more difficult for Victoria Police to manage. The VPDSF's stipulation that approved third parties must offer protection of this information acknowledges this issue and is designed to ensure the data used and stored by third parties is secured.

4.4 Information misuse under-prioritised in investigations

Victoria Police PSC is responsible for investigating suspected misconduct or corruption by Victoria Police employees. For suspected unauthorised access and disclosure of information, PSC investigations often rely on the Information Security and Standards Command (ISSC) to conduct audits of access. However, unauthorised access is often not the primary allegation being investigated, as seen by the low number of allegations of information misuse reported and notified to IBAC. This means that it is sometimes under-prioritised or not pursued in the investigation, with a high focus on the other alleged inappropriate conduct.

This low level of focus on unauthorised access and disclosure in investigations limits not only the full appreciation of the extent of issues, but consequently limits any resulting education or reform. Due to this, there is likely a gap for some employees connecting the importance of information security to integrity.

5 Prevention and detection strategies

IBAC identifies a number of potential measures to assist in preventing unauthorised access of information and disclosure for consideration by Victoria Police and other public sector agencies seeking to strengthen their information management frameworks.

This is not intended to be an exhaustive list and not all the measures will be suitable for all areas of Victoria Police. Public sector agencies have primary responsibility for ensuring the integrity and professional standing of their organisations. Each agency is best placed to fully assess its own risks and operating environment, and to implement the best corruption prevention strategies to address risks.

5.1 Increased, targeted and sustained auditing program

When an auditing program is thorough, proactive and ongoing, it is considered an effective deterrent to employees considering conducting unauthorised checks. However, auditing of police information and data systems can be resource intensive.

A review of procedures for preventing and detecting information misuse, and strengthening of the auditing of systems would assist in a stronger implementation of the VPDSF across Victoria Police.

The majority of LEAP auditing by Victoria Police is considered to be reactive rather than proactive, and relies on reports of wrongdoing. While the LEAP system generates reports of some suspicious activity through warning flag alerts, the number of these alerts is low across the organisation and could be expanded. Additionally, some accountability has been shifted to intelligence practitioners to monitor these alerts. However, this does not address the underlying information security risk and also relies upon intelligence practitioners to act as auditors and question suspicious checks.

The former OPI, Victoria's police oversight agency from 2004 until 2013, conducted a number of investigations into the use of LEAP, and in 2005 found that the auditing of LEAP was resource intensive and costly, with very few results of value (due to LEAP's outdated framework); however, 'a commitment to random and selective audits should be ingrained in [Victoria Police] philosophy'.[44] This suggests that where auditing is difficult, a combination of prevention and detection strategies will be beneficial in increasing information security practices, and preventing information misuse.

An internally publicised targeted auditing program of high-profile cases, including those concerning celebrities and political figures, would help prevent and detect unauthorised accessing of information. Publicising audits would help contribute to building a culture within Victoria Police that believes that if you conduct unauthorised checks, you will be caught.

Victoria Police has advised it is now auditing employees' access following resignation and separation to identify unauthorised access of information which may have occurred. This is partly in response to the perception that employees are less likely to follow proper information security once they know they are leaving Victoria Police. This prevention measure should help to detect unauthorised information access and disclosure by soon-to-be ex-employees and may deter current employees from similar acts.

5.2 Enhanced education and ongoing training

A key strategy for managing any corruption risks within an organisation is the implementation, maintenance and promotion of a sound ethical culture.[45] While a strong, ethical culture is led from the leadership of an organisation, it is important for all employees to be involved in building this culture, including through ongoing communication and training about integrity and why it matters.

Victoria Police has training in place addressing information misuse and security. The PSC Ethical and Professional Standards Officer (EPSO) network across police regions delivers training materials, and the enhancement of this program may make employees more aware that information misuse may be corrupt conduct.

Most training takes places when an employee commences with the organisation and ongoing refresher training is limited, especially for employees who remain in the same position for a number of years. Ongoing training and awareness is essential, as the legislative, regulatory and administrative environments in which the Victoria Police policies operate regularly change.

Due to the complexity of the legislative framework and the VPDSF, clear communication and training is required for employees to be aware of their obligations. An increased focus on training in regional areas (which traditionally see employees stay for a longer time in positions) may increase information security awareness.

Police employees also need specific training on how to deal with the media and journalists in their professional roles and personal lives. This will help mitigate the risks of unauthorised disclosures to media. Basic training for all employees is encouraged to raise awareness around the seriousness and risks associated with leaks to the media. Raising awareness about the criminality of bribery and other inducements to provide police information should also be incorporated into this training.

[45] Standards Australia. *Fraud and Corruption Control 'AS 8001-2008'*, Second Edition 2008, p 14.