Summary

Unauthorised access and disclosure of public sector information

www.ibac.vic.gov.au

Unauthorised access and disclosure of public sector information are forms of information misuse and may constitute corrupt conduct. These activities can also enable other corrupt conduct. This summary highlights common risks across the public sector, the factors that drive information misuse, and outlines strategies to prevent and detect misuse. The full reports are available on IBAC's website[1]. We encourage public sector agencies to review their information management and security strategies in light of these risks.

Key findings

- Unauthorised access and disclosure of information are key enablers of other corrupt behaviour and are often rated as low risk by agencies. Increased understanding that information misuse can enable corruption will help the sector detect and investigate incidents of misuse.
- IBAC intelligence suggests information misuse is underreported across the entire public sector.
- Information misuse is often detected when allegations of other misconduct or corruption are being investigated. An exception to this is the high number of investigations into disclosure of confidential information by the Local Government Inspectorate.[2]
- Unauthorised disclosure to the media is a risk across public sector agencies, and difficult to substantiate as the source of leaks is often hard to identify.
- Sharing information with approved third parties presents corruption risks.
- Increased use of personal devices and smartphones in the workplace has made unauthorised disclosure of information easier. This is particularly the case where public sector employees use personal mobile phones to do their work.
- Unauthorised information access and disclosure is a key risk in procurement.
- IBAC receives more reports of information misuse by Victoria Police compared to other public sector agencies. This may reflect Victoria Police employees and members of the public having a higher level of awareness of the risks related to information misuse by Victoria Police.
- Customised auditing of the information employees can access is underused, and its benefits underappreciated across the Victorian public sector.
- Since being introduced in 2016, the VPDSF/S has shown there is improved public awareness of information security, and data incidents reported to OVIC have increased. The strength of the VPDSS's influence on longer term cultural change will depend on how successfully agencies align their practices with the VPDSF/S.

[1] www.ibac.vic.gov.au

[2] Prior to April 2020, these investigations were under section 77 of the *Local Government Act 1989*. Section 125 of the *Local Government Act 2020* now applies.

Corruption risks

- Unauthorised access for personal interest
- Unauthorised disclosure to media
- Public sector employees targeted for information
- Unauthorised disclosure to benefit associates, including accepting or soliciting bribes
- Politically motivated or 'noble cause' unauthorised disclosures
- Sharing of system login credentials

Corruption drivers

- Personal issues of employees
- Information misuse under-prioritised in investigations
- Information sharing with approved third parties
- Social media use
- High-level access by managers and information technology administrators
- Data analytics and 'big data'
- Aging or weak technology systems
- Social media policy challenges
- Procurement processes
- Elected officials' obligation to keep their communities informed

Prevention and detection strategies

- Increased, targeted and sustained auditing
- VPDSS implementation and increased reporting by public sector agencies
- Enhanced education and ongoing training

ibac independent broad-based anti-corruption commission
Victoria

IBAC has produced three reports on corruption risks related to the unauthorised access and disclosure of information within the Victorian public sector, Victoria Police and local government. While Victoria Police and the local government sector form part of the Victorian public sector, due to the unique risks of each sector, and the associated need for tailored prevention strategies, we produced individual reports on each. For the purposes of this summary, the term public sector applies to all of these bodies.

Corruption risks

IBAC identified common corruption risks for employees accessing and disclosing information without permission. This type of corrupt behaviour can be due to individual decisions and actions, as well as insufficient controls and systems.

Unauthorised access for personal interest

Many public sector employees have access to large volumes of information which can be highly valuable to private or criminal interests. While the amount of classified or otherwise sensitive information held by agencies varies, most agencies manage information which could be targeted for illegal or corrupt means. For example, Victoria Police holds information on nearly all members of the public (including addresses, phone numbers, criminal histories and driver licence information), while local councils hold some of this personal information as well as planning and property development information.

Unauthorised disclosure to media

The media plays an important role in shaping the relationship between government and the community. In fact, public sector agencies often rely on the media to communicate information that is in the public interest. However, unauthorised disclosures to media is a common allegation received by IBAC, and challenging to investigate. It is often difficult to identify who disclosed the information given the large number of employees with access to it, and due to the important legislative protections that journalists and their sources have. Public sector agencies that manage high-profile public interest matters are at heightened risk.

Public sector employees targeted for information

IBAC investigations have shown repeated instances of public sector employees unlawfully disclosing information to associates, often for criminal purposes and financial benefit. These types of investigations are more commonly in relation to police employees as IBAC has a lower threshold for investigating police misconduct in comparison to public sector corruption. However, IBAC has conducted a number of similar investigations in relation to employees of local government and the corrections sector.

Public sector employees can be targeted due to their general access to information, not necessarily due to their individual roles or units where they work. This targeting can take place by friends and family, or by others known to them. Criminals can 'befriend' employees with the aim of using them to access information (known as grooming). Many employees have access to sensitive and official information, so it is difficult to detect employees who may be targeted and offend.

Unauthorised disclosure to benefit associates, including accepting or soliciting bribes

Unauthorised information disclosure to associates is a common theme across IBAC investigations and a key enabler of other corrupt conduct. In IBAC investigations of police and public service agencies, bribery and kickbacks have not featured as a motivation to date for unauthorised information release – rather, it has been more commonly seen to occur either as a favour or act of goodwill. Comparatively, health, human services and corrections sectors are at higher risk due to the personal information they hold, along with agencies that manage political and financial information due to the consequences of this type of information being leaked.

IBAC commonly receives allegations against local government employees and councillors relating to bribes in exchange for information. This has been particularly evident in planning and development matters, likely due to the greater financial benefits arising from access to this information.

Politically motivated or 'noble cause' unauthorised disclosures

Some public sector employees regularly engage with political and community groups as part of their role, while others do this in their private lives. Formal liaison between public sector agencies and these groups is often essential for community safety and to inform government decision-making. However, this creates risks of unauthorised disclosures as these relationships rely on frequent exchanges of information.

The issue of politically motivated unauthorised disclosures has been highlighted to IBAC during consultations with the public sector, suggesting it is a risk across IBAC's jurisdiction. For Victoria Police, high-profile criminal cases are of specific risk, with IBAC receiving reports of unauthorised disclosures by Victoria Police employees to their friends, family members and the media. For local government, these types of disclosures are more likely to occur during elections or be related to council decision-making.

There are also instances where disclosing information is motivated by a 'noble cause'; what the individual considers ethical reasons. Although these disclosures are driven by good intentions, they may still be unlawful or in breach of policy (unless otherwise made under the *Public Interest Disclosure Act 2012 (Vic)*).

Sharing of system login credentials

Unauthorised access of information also occurs when an employee uses another employee's login details to access information. IBAC intelligence suggests this occurs more frequently in offices where desk sharing takes place, most commonly in regional areas or in offices doing field work. This makes it difficult for public sector agencies to detect and prosecute information misuse when it does occur.

IBAC intelligence suggests that support staff, particularly executive assistants, frequently use systems under executives' login details and passwords. This presents a number of risks and creates difficulties in detecting unauthorised access or disclosure.

Corruption drivers

Public sector agencies manage different types of information. Due to this, corruption risks vary across public sector agencies and have different drivers. Accordingly, public sector agencies are best placed to identify and manage their own unique corruption drivers and risks.

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. Such issues can include alcohol and drug abuse, breakdowns in personal relationships, gambling or instances of physical or mental illness. IBAC notes many public sector agencies have employee assistance programs which, if effectively promoted and accessed by employees, may help reduce the risk of information misuse.

Information misuse under-prioritised in investigations

Many public sector agencies conduct their own investigations into allegations of employee misconduct or corruption. Information security areas are often relied upon to conduct audits of access for suspected unauthorised access and disclosure of information. However, as seen by the low number of allegations of information misuse reported and notified to IBAC, unauthorised access is often not the primary allegation being investigated by public sector agencies or IBAC. This means this type of conduct is sometimes under-prioritised or not pursued in an investigation due to a greater focus on other alleged inappropriate conduct.

A low level of focus on unauthorised access and disclosure in investigations impacts upon an agency's ability to fully appreciate its prevalence or pursue any subsequent education or reform. Due to this, gaps are likely to exist in employees' awareness of the important link between integrity and information security.

Information sharing with approved third parties

Public sector agencies frequently share information with approved third parties, including other public sector and law enforcement agencies in Victoria, across Australia and sometimes overseas. Under the *Privacy and Data Protection Act 2014 (Vic)* (PDP Act), a public sector body head (such as a Secretary or Chief Executive Officer) must be assured that approved third parties will offer the same, or better, protection of information.[3] However, intelligence suggests that due to limited detection and auditing by public sector agencies, unauthorised information access and disclosure of confidential information by third parties remains an issue, particularly for Victoria Police given the amount of information it holds of a sensitive and confidential nature.

[3] PDP Act Section 88 (2) states "*A public sector body Head for an agency or a body to which this Part applies must ensure that a contracted service provider of the agency or body does not do an act or engage in a practice that contravenes a protective data security standard in respect of public sector data collected, held, used, managed, disclosed or transferred by the contracted service provider for the agency or body.*"

Social media use

Social media users, including public sector employees, are able to upload large amounts of personal information and opinions to both public and restricted social media platforms. Many public sector agencies recognise the risks associated with social media and have a policy to manage this. However, public sector agencies continue to face integrity issues related to social media, including the use of these platforms to discuss work activity.

IBAC has identified many public sector employees will use social media platforms to communicate with colleagues, often to discuss work related topics. Although in many cases access to these platforms is password protected, employees may not appreciate that the information they upload is at risk, or that the social media platform now 'owns' the information. Using social media and encrypted platforms to communicate also increases the risk of official information being leaked by employees without detection.

High-level access by managers and information technology administrators

Compared to other employees, managers and supervisors often require a higher level of access to information systems to fulfil management responsibilities. This can include access to confidential personal details in human resources, payroll and financial systems, as well as information specific to their agency. This high-level access can drive unauthorised access to information and lead to personal benefits.

Employees working in information technology with high levels of access present greater information misuse risks. They often work with a high level of autonomy and little oversight, and possess skills that could be used to cover up misconduct.

The public sector often competes with the private sector for information technology specialists. These employees frequently bring new skills and innovation to the public sector. IBAC has seen recurrent trends of public sector agencies hiring specialists as contractors in order to compete with the salaries offered in the private sector. A key implication of this is that contractors from outside the public sector may not have professional values and ethics aligned with the VPS Code of Conduct, or may not receive the required standard of training for an employee with high levels of access to official information.

Data analytics and 'big data'[4]

There are known corruption risks with data analytics and 'big data', as they combine previously separate datasets into a new database for matching. While this capability can provide beneficial outputs to public sector efficiency and effectiveness, it can also allow employees to access information which they previously may not have had access to, and increases the value and sensitivity of the data as it is matched with new related information. For example, data analytics outputs may combine multiple pieces of personal identifying information, such as details of driver licences, addresses and bank accounts, which potentially increases the consequences when this information is misused.

[4] There is no definitive definition for big data; however, the Office for the Australian Information Commissioner refers to a common definition of 'high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight, decision making, and process optimization.' Office for the Australian Information Commissioner, Consultation draft: Guide to big data and the Australian Privacy Principles, May 2016.

Aging or weak technology systems

Aging systems can limit the ability to securely access and disclose information within agencies and approved third parties. Systems that encrypt data and quickly share information are now commonly used throughout society. However, certain areas of the public sector have not been able to adopt these technological advances and provide these services, potentially limiting information security.

Social media policy challenges

Policies surrounding social media and smartphones across the public sector vary, with some agencies having guidelines and others having dedicated policies. A lack of policy, or poor policies and guidelines, may contribute to the misuse of information on social media because employees are unaware of their responsibilities in handling information. Additionally, there is an ongoing challenge to keep policies up-to-date and in line with technological advancements.

Procurement processes

Financial management, including procurement processes, vary across the public sector. In local government, the *Local Government Act 2020 (Vic)* offers guidelines rather than prescribed governance arrangements. The lack of uniform governance across individual councils may leave gaps in how procurement processes and information sharing is managed. A procurement valued less than $10,000 is known as small-value procurement, and has flexible policies which can often be interpreted to suit specific situations. This has been highlighted to IBAC as a key vulnerability for local government as it means information management during small value procurement, including access and disclosure, may not be subject to the same levels of oversight as across the rest of the public sector.

Elected officials' obligation to keep their communities informed

Elected officials in state and local government, including councillors, must balance being transparent to their constituents with securing official information.

IBAC intelligence suggests some councillors face challenges in managing this balance. These challenges are more likely to arise for councillors, as opposed to local government employees, due to a lack of awareness of the legislation and requirements relating to information disclosure and decision-making protocols. This is especially the case for recently elected councillors.

Legislative requirements around information security in Victoria

The Office of the Victorian Information Commission (OVIC), in its role as independent regulator with combined oversight of information access, information privacy, and information security, administers the PDP Act. Part 4 of the PDP Act (Protective Data Security), requires OVIC to develop the Victorian Protective Data Security Framework (VPDSF) for monitoring and assuring the security of public sector data. Additionally, OVIC may issue protective data security standards (VPDSS). The framework and standards were originally issued in 2016, and were updated in 2019/20.

Application of the framework and security standards helps to prevent and detect information misuse and other breaches of information security. It applies to the majority of public sector agencies and bodies in Victoria.

While Part 4 of the PDP Act does not expressly apply to local government, there are technical exceptions that result in most local councils having obligations to implement the VPDSS. OVIC recommends local government establish a monitoring and assurance program in accordance with the obligations outlined in the VPDSF. In addition, by implementing the VPDSS councils would strengthen and standardise information security practices. For more information, visit OVIC's website.[5] Breaches of information security are encouraged to be reported to OVIC.

[5] www.ovic.vic.gov.au

Prevention and detection strategies

IBAC's research identifies potential measures to assist in preventing unauthorised access and disclosure of information for consideration by public sector agencies, especially those seeking to strengthen their information management frameworks. This is not intended to be an exhaustive list, and not all measures will be suitable for all agencies. Each agency has an in-depth understanding of its own work practices and organisational culture and is best placed to assess its own risks, and implement the most effective corruption prevention strategies.

Increased, targeted and sustained auditing

When an auditing program is thorough, proactive and ongoing, it can effectively deter employees from conducting unauthorised checks. Many audits across the public sector are reactive rather than proactive, as they rely on reports of wrongdoing. While auditing information and data systems can be resource intensive, strengthening auditing systems would assist in implementing the VPDSS across the public sector.

For agencies that hold citizen's personal information, undertaking internally publicised and targeted auditing programs of employees' access of high-profile people, including celebrities and political figures, would help prevent and detect unauthorised accessing of information.

Publicising audits would strengthen the culture and understanding across the public sector that employees will be caught if they conduct unauthorised checks.

Victoria Police advised IBAC that it is now auditing employees' access to information during the notice period after an employee has submitted their resignation. 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 detect unauthorised information access and disclosure by soon-to-be ex-employees and deter current employees from similar acts. This strategy could be adopted by other agencies facing similar risks.

VPDSS implementation and increased reporting by public sector agencies

Good information management promotes good information security. The VPDSF outlines monitoring and assurance obligations for organisations. The VPDSS provides strong information security standards for the public sector, which, if fully implemented, is likely to significantly strengthen and standardise information security practices across the VPS. The VPDSS will have flow-on effects leading to better practices in auditing and compliance, as well as assure the community that official information held by the public sector, including citizens' personal details, is secure.

Enhanced education and ongoing training

IBAC understands there is a general under-appreciation for information management and a lack of awareness of how information misuse can constitute – but also enable – corrupt conduct. Due to the complexity of information management requirements in Victoria, increased training in legislative requirements for handling official information and data is expected to assist in better practice. OVIC, the Public Record Office Victoria (PROV), and the Enterprise Solutions Branch within DPC provide online education and deliver face-to-face training when requested. Many public sector agencies require employees to undergo induction training for information management, often completed through online modules, and there is scope to include training from OVIC and PROV.

Increased and regular training should also include education on the serious consequences associated with information misuse. Greater use of case studies of offending, where investigations have led to contracts being terminated or other punitive action, could also encourage a greater understanding of risks and may deter future offending. Public sector agencies also have an obligation to manage the ongoing suitability and eligibility of all persons with access to official information. This should be supported by a regular program of review that tests and confirms ongoing suitability.

Links and other useful resources

Independent Broad-based Anti-Corruption Commission

Research report: *Unauthorised access and disclosure of information held by Victoria Police*

www.ibac.vic.gov.au/publications-and-resources/article/unauthorised-access-and-disclosure-of-information-held-by-victoria-police

Research report: *Unauthorised access and disclosure of information held by the Victorian public sector*

www.ibac.vic.gov.au/publications-and-resources/article/unauthorised-access-and-disclosure-of-information-held-by-the-victorian-public-sector

Research report: *Unauthorised access and disclosure of information held by local government*

www.ibac.vic.gov.au/publications-and-resources/article/unauthorised-access-and-disclosure-of-information-held-by-local-government

Case studies

Operation Genoa

www.ibac.vic.gov.au/publications-and-resources/article/case-study---operation-genoa

Office for the Victorian Information Commissioner (OVIC)

Victorian Protective Data Security Framework

ovic.vic.gov.au/data-protection/framework-vpdsf/

Victorian Protective Data Security Standards

ovic.vic.gov.au/data-protection/standards/

Frequently asked questions

ovic.vic.gov.au/data-protection/for-agencies/frequently-asked-questions/

Public Record Office Victoria (PROV)

Standards framework: Under the *Public Records Act 1973 (Vic)*, the Keeper of Public Records is responsible for the establishment of mandatory Standards for the efficient management of public records

prov.vic.gov.au/recordkeeping-government/about-standards-framework-policies

Queensland Crime and Corruption Commission

Operation Impala: In 2019 the Crime and Corruption Commission launched Operation Impala to examine the improper access and dissemination of confidential information by public sector agencies in Queensland.

www.ccc.qld.gov.au/public-hearings/operation-impala

Level 1, North Tower
459 Collins Street,
Melbourne VIC 3000
GPO Box 24234,
Melbourne, VIC 3001

T 1300 735 135
F (03) 8635 6444

December 2020

IBAC is Victoria's anti-corruption agency responsible for preventing and exposing public sector corruption and police misconduct. We do this by:

- investigating serious corruption and police misconduct
- informing the public sector, police and the community about the risks and impacts of corruption and police misconduct, and ways in which it can be prevented.

To report corruption now, visit **www.ibac.vic.gov.au** or call **1300 735 135**.

If you need help with translation, call the Translating and Interpreting Service on **13 14 50** or visit **www.ibac.vic.gov.au/general/accessibility/tr**