VICTORIA

Victorian
Auditor-General

Audit summary of Maintaining the Integrity and Confidentiality of Personal Information

Tabled in Parliament
25 November 2009

Audit summary

Background

The public sector is a complex business. In its normal, day-to-day activity it legitimately gathers and uses personal information about citizens, and shares it with a range of entities both within and outside government.

Personal information is information about an individual that identifies a person. Information such as your name and address may be readily accessible, and well known within the community. However, other information, such as your health or criminal record, may not be well known and should not be easily accessible.

This report examines how personal information is stored, processed and communicated by the public sector. It evaluates whether its confidentiality and integrity has been maintained.

Maintaining confidentiality means that personal information is accessed only by those who need it to perform their duties. Maintaining integrity means that information provided is not later corrupted or lost, either intentionally or inadvertently.

Personal information can be misused with potentially serious consequences. For example, an individual can suffer financial loss or damage to their credit rating, their medical records can be compromised, or they may suffer from threats, and/or harassment if their identity is ‘stolen’. To redress the damage, a person may also suffer loss of time and money.

Effective information security controls that focus on safeguarding all information and information systems are needed. Securing information, including personal information, requires a balanced and integrated approach to people, process and technology, with a strong security governance framework.

This report assesses whether governance and risk management practices in three departments have been sufficient, and whether central policy direction and guidance has effectively driven the public sector to achieve this aim.

Overall conclusions

The confidentiality of personal information collected and used by the public sector can be, and has been, easily compromised. While we examined only three departments, the ability to penetrate databases, the consistency of our findings and the lack of effective oversight and coordination of information security practices strongly indicate that this phenomenon is widespread. Recent incidents of personal information being found in public places or in the hands of unauthorised persons, are further evidence of this.

This situation has arisen partly because information security policy, standards and guidance for the sector are incomplete and too narrowly focused on ICT security.

The central direction and effective coordination of the broad scope of information security risks remains weak. Neither the Department of Treasury and Finance nor the Department of Premier and Cabinet have addressed all aspects of information security following the disbanding of the Office of the Chief Information Officer and its supporting committees in 2006.

In the absence of strong and consistent central leadership and effective oversight, the importance of protecting personal information has not been properly understood by the sector. The departments examined have recently strengthened their information security governance, but information security risks have not been managed effectively. Elements of organisational culture, practices and controls all have weaknesses that can be exploited to breach confidentiality in the systems examined. There is also little assurance that the integrity of data has been maintained in these systems.

Weaknesses in controls over the confidentiality and integrity of financial information have been identified through our annual financial audits and reported to the Parliament for many years. It is disappointing that the important lessons about security of information also translate into non-financial information.

Main findings

Governance

The way in which the Victorian public sector does business is increasingly sophisticated and the relationships it develops, increasingly complex. The exchange of information with other agencies, the private sector and across jurisdictions creates a range of challenges such as, who owns the information, how can recipients be directed to provide equivalent standards of privacy and security over the information shared, and who is responsible if the information is lost or leaks and confidentiality is breached.

The approach to managing information security has not met these challenges or kept up with how the sector does business nor the complexity of its business relationships.

It is imperative that action is taken quickly to provide more effective governance and leadership so that these situations are remedied.

The Department of Treasury and Finance and the Department of Premier and Cabinet have not fulfilled their responsibilities to develop and maintain whole-of-government information security standards and guidance, to improve the coordination of identity and information management systems at state level, and to provide policy advice on emerging trends and issues in identity and information management.

Under the state's governance arrangements, responsibility and accountability for departmental performance rests with departmental secretaries. However, our findings from within three departments, and our wider discussions in the sector, demonstrate that departments and the wider public sector need better direction about information security and management. More timely development of standards and guidance relevant to local conditions and risks is needed; as is better identification and effective management of risks, including emerging whole-of-government risks; better education and awareness-raising across the sector; and allocation of resources to achieve the minimum standard required.

Most public sector agencies are currently not mandated to comply with public sector information security policy and standards. Given that information is legitimately shared by agencies throughout the sector, this has the potential to compromise the mandated information security arrangements in place in departments.

Culture, practice and technology

Fundamental flaws are evident in the way the Victorian Government Risk Management Framework is applied, and greater guidance across the sector is needed. Risks cannot be managed where an agency is not aware of them, or does not understand their significance. Without substantiation, attestations by agency heads about the effectiveness of controls have no value.

Information security risks were not effectively managed within the three departments. In one, threats to and vulnerabilities of the systems and networks were understood within the information technology section but advice had not made its way to senior management and so were not effectively managed. Similarly, in the two other departments, business units were aware of the risks to the information but the risks were not uniformly managed across the department.

Databases that stored personal information could be accessed by unauthorised people, quickly and easily. This was because the information was not appropriately classified and the necessary controls were either missing, or were not operating as required.

Departments could not be sure their systems had not previously been breached and personal information accessed by unauthorised parties or stolen, because logs of access and changes were either not maintained or not reviewed on a timely basis.

Since the audit the departments have acted to improve security over the databases examined.

Data was transmitted from the three departments by emails in formats that were easily read. This means they could be accessed by someone other than the intended recipient.

Personal information was stored on portable storage devices, CDs and DVDs that are vulnerable to loss, in easily-read formats. Personal information was exchanged via personal email accounts, some of which were particularly vulnerable to unauthorised access. Extracts or whole copies of personal information from the selected databases were stored in unsecured shared drives on departmental networks accessible by unauthorised staff. Compliance by staff with information security requirements was not monitored by any of the three departments.

All three departments provide personal information to third parties—organisations that provide services on their behalf; that provide ICT services; or that host their information systems. Departments did not require independent certification, or carry out their own assessment, that the security third parties had in place met the required public sector security standards. There was little assurance that information was adequately protected by third parties to whom the information was legitimately provided.

Recommendations

Number	Recommendation	Page
1.	The Department of Treasury and Finance and the Department of Premier and Cabinet should: • clarify their respective roles and responsibilities for information security, to better coordinate their activities, and to address the functions of the disbanded OCIO and its supporting committees • expedite the release of a comprehensive, integrated suite of standards and guidance that address all aspects of information security including protective security, and which are based on risk and relevant to local conditions • mandate that all public sector agencies adopt the whole-of-government information security policies and standards • establish clear oversight to monitor implementation of information security policies and standards and compliance with the reporting requirements • establish a process to identify and communicate emerging information security risks to the sector.	16
2.	All public sector agencies should assign responsibility for information security practices both to senior management, and to line management at appropriate levels throughout the organisation.	16

Recommendations – *continued*

Number	Recommendation	Page
3.	To adequately protect the integrity and confidentiality of citizens' personal information each public sector agency should: • Develop more robust risk management practices, which demonstrate that annual risk attestations are based on substantiated evidence that information controls are effectively addressing risks. • Include in staff training, the importance of information security; the range of threats to information security and the vulnerabilities of electronic and hardcopy records and physical security in workplaces. • Regularly monitor compliance by staff with information security policies, standards and required practices. • Conduct an inventory of all the information they store, process and communicate, assess its criticality, classify the information; and determine, and put in place, the minimum controls needed to protect it. • Assess the threats and vulnerabilities, both internal and external, to their ICT systems, implement appropriate controls to address them and regularly monitor that the controls are in place and operating as required. • Regularly monitor logs and records of access and changes to information. • Establish agreements with third party service providers to clearly specify minimum standards of security over information handled, at least equal to those required of the public sector, and that provide for regular certification of compliance with the standards. • Conduct periodic random checks of the controls in place at third party service providers over citizens' personal information.	26