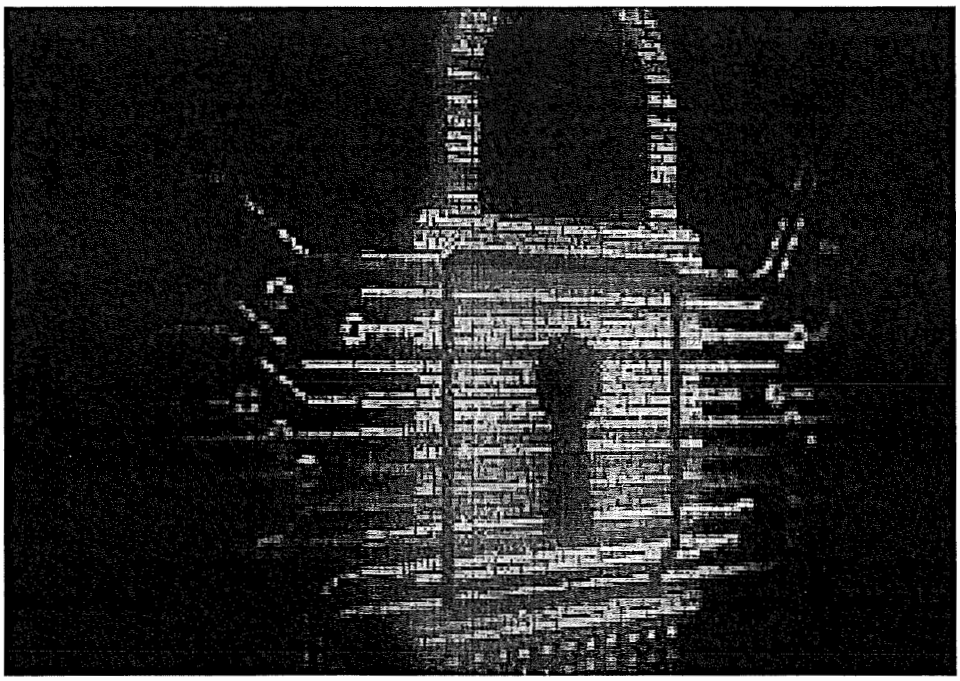
WA POLICE

Professional Standards Portfolio

INFORMATION INTEGRITY PATHWAY / ROADMAP FOR REFORM



IPAA WA Public Sector Research Day 2016

An informing paper by Senior Sergeant Ceri Skamp

INTRODUCTION

The Western Australia Police (WA Police) is the owner and user of multiple computer systems, many of which hold a vast array of private and confidential information. All of these systems, regardless of their content, constitute a Restricted Access Computer System (RACS) as defined in section 440A of the *Criminal Code Compilation Act 1913* (CC)[1]. The integrity and security of information contained within these systems is of paramount importance, and the general public has an expectation the information is only accessed by authorised persons in a lawful and appropriate manner.

An extensive suite of computer firewalls protect the information from external access via computer 'hackers'. This is an on-going risk which is managed and mitigated on a daily basis. However, an equal and more complex risk exists from the threat of WA Police employees (and other authorised users) who access RACS in the course of their employment and then go beyond their remit and use them beyond their authorisation. The governance and policing of WA Police authorised users is highly refined, but despite these measures, breaches of RACS occur on a weekly basis.

This paper deals with the current effectiveness of the WA Police deterrence, prevention and detection strategies for all WA Police users, including authorised external users from other agencies. The paper also provides recommendations to improve security and governance to ensure compliance by WA Police members.

To instigate these changes the WA Police will be required to implement a clearly defined Information Integrity Pathway (IIP) to deliver structural changes, supporting processes and technologies. The core of the IIP is to initiate a change of culture to move from a perception of ownership of information to one of being a 'custodian' of the information. Changing the culture within any agency is the most challenging endeavour of this initiative and requires a consolidated and concerted approach over a lengthy period of time.

The study has identified a number of synergies with other government and non-government agencies and could be a leading example to develop multi-disciplinary collaboration and innovative use of contemporary information technologies.

[1] *Criminal Code Compilation Act 1913*

1.0 HISTORICAL CONTEXT / BACKGROUND

As early as 1997 police jurisdictions outside of Western Australia were identifying problems relating to improper and unlawful use of RACS, and these formed a common theme amongst Royal Commissions in Australia. Additionally, it was found computer misuse was rarely a stand-alone issue and was linked to other, often more serious unprofessional conduct.

In January 2004, the final report of the Kennedy Royal Commission[2], Chapter 11 was dedicated to solely to the topic of computer misuse. The following paragraph articulated the broader issues which were discussed:

'*The need to ensure the confidentiality of personal information and integrity in the use of the information is important in maintaining public confidence in WAPS. There is a broad public awareness and concern about the amount of personal information that is being stored by government instrumentalities. In respect of the police there is an acceptance that police officers should have access to such information in order for them to carry out their work effectively and expeditiously. On the other hand, members of the community increasingly need assurance that their confidential information will be used only for proper policing purposes, and that their rights to privacy will be respected*'.

The Kennedy Royal Commission found '*unauthorised access of WAPS information databases has continued to occur in a variety of circumstances and with varying degrees of harm flowing*' and further stated '*WAPS needs to substantially improve its system for control of access to information collected by it, and take stronger action, including prosecution, when breaches of its procedures are detected*'.

The majority of the recommendations were embraced and implemented by the WA Police but computer misuse still continues to this day.

2.0 COMPUTER MISUSE / GENERAL FACTS

The threat of information being obtained and used unlawfully is divided between external threats (via hacking) and internal threats from authorised users who act beyond their mandated authority. There are a myriad of IT (Information Technology) solutions utilised by the WA Police to implement effective firewalls to prevent hacking. These systems are complex and reliant on an ever changing threat perspective and technological advances.

[2] Royal Commission into whether there has been corrupt or criminal conduct by any Western Australia police officer.

There are no reliable statistics which accurately reveal the true extent of computer misuse within any agency in Australia. Most meaningful data is derived from statistics of members who have been caught for computer misuse and this is a highly under-representative measure at best. The extent of misuse is dependent on the combination of a number of variables which include, but are not limited to the following:

- The culture of the agency in how members collectively appreciate the proprietary of accessing of private information.
- The induction and on-going training of staff to re-enforce their knowledge of the rules pertaining to the access of information.
- The sophistication and implementation of various IT solutions to prevent and deter members.
- The manner in which the RACS are constructed and the levels of security within each system.
- The complexity of the tools available to properly audit systems.
- The tenacity of the organisation to pro-actively identifying and deal with misuse.
- The type of information retained in the systems.
- The relevant policies & procedures which articulate how information may be accessed.
- The outcomes for members who have engaged in computer misuse and its general deterrence effect.

All State and Federal Law Enforcement Agencies utilise RACS to secure sensitive data.

In a report in November 2000 by the Queensland Criminal Justice Commission[3] it stated '*However, it is clear that complaint statistics should not be relied upon as an accurate measure of prevalence for this type of misconduct, nor should the complaints' mechanism be considered a comprehensive system of monitoring and detecting improper access and/or release of confidential information'.*

In a detailed report by the Western Australia Corruption and Crime Commission[4] (CCC) published in September 2005 it stated '*The exact extent of the problem of misuse of computer systems through unauthorised access and disclosure is not known and it is widely suspected that a great deal goes undetected,* and further, *'all we are ever seeing is the tip, and the iceberg itself remain largely unseen and unknown.*

This paper proposes computer misuse falls into three broad categories (regardless of which agency owns the RACS) namely:

[3] Queensland Criminal Justice Commission 'A report on the improper access to, and release of, confidential information from the police computer systems by members of the Queensland Police Service.
[4] Corruption and Crime Commission[4] CCC 'An inquiry into unauthorised access and disclosure of confidential information held on the electronic databases of public sector agencies'.