Answer to question taken on notice by Dr Waldersee

Much cybercrime activity is associated with organised criminals using software to attack organisations, which is the purview of organisations such as the AFP, and NSW and Australian Crime Commissions rather than the ICAC. However most definitions of cybercrime also include the broader misuse of ICT. The ICAC is aware of instances of the misuse of the ICT systems within public agencies for corrupt purposes.

More often than not these matters relate to the administrative control of ICT systems rather than technical manipulation of the hardware or software. These administrative matters can include the failure to revoke passwords at the right time, password sharing, absence of firewalls and so on. Such misuse has been observed in a number of public inquiries, including Operations Hunter, Monto and Carina. In those investigations, corruption prevention recommendations concerning ICT systems were made to the relevant agencies.

The corruption prevention division has also provided guidance to agencies concerning how their ICT systems should be set up and managed to reduce the risk of corrupt conduct occurring. For instance, the corruption prevention section of the ICAC's website contains a page on managing ICT systems. The division has also produced a publication and delivered presentations on how to manage ICT projects and engage ICT contractors, as these are the genesis of many failings in ICT systems. Finally, agencies' financial systems and the administration of the ICT systems involved in financial systems are one key area being considered by the division's current project into invoice payment.