

Information Systems Audit Trails; An Australian Government Survey

Caroline Allinson

Manager Information Security, Information Management Division,
Queensland Police Service, GPO Box 1440, BRISBANE Qld 4001, Australia.
and
Information Security Research Centre (ISRC),
Queensland University of Technology, Brisbane. Queensland. Australia.

Governments have major information holdings on computer systems. This electronically stored information is subject to legislative requirement. However, history has shown that security in relation to the recording of activity against access to information held on Australian government computer systems has been poor and a cause for concern.

A brief definition of information systems audit trails is given, with emphasis on national and international standards requirements. Aspects of Australian privacy legislation are discussed.

Background, detail and results of an Australia wide survey of all government departments is given and contrasted with particular results of a survey conducted by the Australian Commonwealth Privacy Commission four years previous.

It is shown that most organisations studied generate and retain audit trails but the approach is not consistent nor is it comprehensive. Within a four year period there is evidence to suggest that government organisations are increasingly more inclined to generate audit trails. It is also suggested that due to the inadequate and non-compliant security processes and procedures these materials would not withstand a serious legal challenge.

Keywords: Audit-Trails, Evidence, Information-Security, Policy, Survey, Computer.

1. INTRODUCTION

In a computing environment an audit trail supports a management control aimed at enforcing user and system authentication and authorisation. This is achieved by making and keeping, secure records of all necessary information system activities. Two motivating factors for the use of audit trails in the current environment are detection of unethical/unauthorised behaviour and demonstration of a 'proof of business process'. These two factors may include such activities as exceeding access control rights, inappropriate and illicit release of information, correct adherence to required business procedures and fraud prevention (Allinson, 2001). An audit trail record may contain a description of an event/activity, the date and time of the event/activity, the identity of the

Copyright© 2002, Australian Computer Society Inc. General permission to republish, but not for profit, all or part of this material is granted, provided that the JRPIT copyright notice is given and that reference is made to the publication, to its date of issue, and to the fact that reprinting privileges were granted by permission of the Australian Computer Society Inc.

Manuscript received: April 2001
Associate Editor: John Roddick