Edith Cowan University
Research Online

Australian Information Warfare and Security Conference

Conferences, Symposia and Campus Events

2006

A study of the compliance of alarm installations in Perth, Western Australia: Are security alarm systemsbeing installed to Australian Standard AS2201.1 - "systems installed in a client's premises."

Robert E. McLaughlin
Edith Cowan University

David J. Brooks
Edith Cowan University

DOI: 10.4225/75/57a8123aaa0cd
Originally published in the Proceedings of 7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/isw/14

A study of the compliance of alarm installations in Perth, Western Australia: Are security alarm systems being installed to Australian Standard AS2201.1 – "systems installed in a client's premises."

Robert E. McLaughlin
David J Brooks
School of Engineering and Mathematics
Edith Cowan University
International Centre for Security and Risk Sciences
r.mclaughlin@ecu.edu.au
d.brooks@ecu.edu.au

Abstract

This study presented an overview of the training available to intruder alarm installers. A survey of domestic and commercial intruder alarm systems (n=20) were completed across Perth, Western Australia, metropolitan area. The gathered data were evaluated against Australian Standard AS2201.1 for intruder alarm systems, to determine whether alarm installations comply with two parts of the standard, being that of control panel location and zone supervision. AS2201.1 requires that intruder alarm control equipment shall be located within the alarmed area, located outside the entry/exit point and operate as dual end-of-line supervision. The study presents significant findings into the compliance of installed intruder alarm systems. A significant proportion of the intruder alarms measured did not comply with AS2201.1, with the panel located outside an alarmed area (30%), located in the entry/exit point (15%) and not capable of dual end-of-line supervision (30%). These items contravene Australian Standard AS2201.1. Assumptions suggest that non-compliance is due to a lack of industry focused vocational training, industry self regulation and supervision, licensing regime and legislation. No single aspect could be considered ineffective; rather it is argued that all of these areas need to be addressed.

Key words
Intruder alarms, legislation, compliance, training, awareness

INTRODUCTION

In all states of Australia, State Police Services through legislation provide a level of control of the security industry and their services. Control is achieved through licensing arrangement, based on technical understanding and quality of character (Commercial Agents Unit, 2006). Intruder alarm systems form an integral part of security. But it could be suggested that consumers have limited awareness in the quality of installation and technical understanding of these systems. These issues leave the consumer prone to poorly installed or non-compliant intruder alarm systems, if licensing is ineffective.

Background

As an industry, "security" has had rapid growth (Hemmens, Maahs, Scarborough & Collins, 2001). In a recent study, census figures for a five-year period, 1996 - 2001 showed that while the Australian population increased by 6.0%, and the police industry workforce by 6.5%, the number of security providers grew by 31.1%. It could be suggested that the public is now highly dependent on security services, but current issues suggested the need for more sophisticated regulation to improve conduct and quality of service (Prenzler, 2005).

Security installers provide electrical and electronic security systems for domestic premises and commercial businesses, as well as 24 hour backup service, maintenance and repairs. These systems include burglar alarms, closed circuit television systems (CCTV), access control systems and security lighting. Much of this equipment is computerised and highly sophisticated, with updates and new versions being released on a regular basis. It is suggested that to keep abreast of new trends, some form of regular training is necessary.

Of the 1400 security installers licensed in Western Australia (Table 1), 291 installer licenses were issued in 2005.
Table 1
Western Australia installer licenses

Licenses issued during 2005 (up to 30/11/05)	
Security Agent	177
Consultant	226
Installer	291
Officer	2,183
Overall current license numbers (up to 30/11/05)	
Security Agent	1,028
Consultant	1,327
Installer	1,431
Officer	7,669

(Acting Senior Sergeant S. Wood, personal communication, December 1, 2005)

Installer training and testing

The alarm test Security Installers must complete prior to being licensed to install or maintain electronic alarm systems is based on Australian Standard AS2201.1 (Intruder Alarm Systems). Also tested are basic electronics skills, including circuit calculations and component values. The total test requires a minimum 80% pass rate (Commercial Agents Unit - Pre-License Requirements, 2003).

The Balga campus of Technical and Further Education (TAFE) in Western Australia provides a Certificate II course in Electro-technology Servicing (Security Systems). Successful completion of this course provides students with the knowledge and preparation to undertake a security installer's license examination, conducted by the West Australian commercial agent's branch. With approximately 90% of Western Australia security system installers working in the Perth metropolitan area, Balga TAFE is the only provider of this course in Perth (Department of Education and Training, 2006). In 2000, approximately 70 people commenced the Certificate II in Electronics (Security System Installation). In 2005, 31 students attended the course (D. Fleay, personal communication, November 23, 2005), although 291 new installer licences were issued (Table 1).

Education usually refers to learning in an academic environment. Training is more industry specific. Training teaches procedures that help individuals meet professional goals and perform better on the job (Keller and Chuvala, 1992, p. 102). Education can be provided through universities and technical colleges such as Curtin University of Technology, Edith Cowan University, Swan TAFE and West Coast College of TAFE. Industry associated magazines and journals may also provide articles on new technologies or knowledge gained by technicians in the field. Training can also be provided via professional bodies, government agencies, allied industries, wholesalers and equipment suppliers, supervisors and managers.

STUDY OBJECTIVES

The objectives of this project were to study the compliance of alarm installations in Perth, Western Australia against the requirements of Australian Standard AS2201.1 for intruder alarm systems. The study determined whether alarm installations are meeting two basic standards, being control panel location and zone supervision.

The study objectives were to:

1. Review the training options available to security installers in Western Australia.
2. Determine the knowledge required to be licensed as a security installer in Western Australia.
3. Conduct a series of on-site intruder alarm system evaluations across the Perth metropolitan area. The evaluations considered two questions regarding compliance with Australian Standard 2201.1 -'systems installed in a client's premises':
    a) Is the security control panel sited within a protected area?
    b) The type of zone input supervision, being single or dual end-of-line resistance?
4. Measure the degree of compliance with current standards.

On completion of the study, it was expected that a valid and reliable cross sectional percentage of Perth intruder alarm systems are measured for AS2201.1 compliance within the context of the two questions. As a valid sample, the study determined how well alarm installers comply with Australian Standard AS2201.1 for their alarm

installations. Assumption will be presented that consider why these systems are not being installed to an appropriate degree.

Research Questions

The purpose of the study was to measure the compliance of intruder alarm systems, with the research questions being:

1. Are domestic and commercial intruder electronic alarm systems being installed as per AS2201.1?

2. When compared to AS2201.1, what measures of compliance are domestic and commercial intruder electronic alarms systems being installed to?

The significance of the study was to measure whether intruder alarm installers had learnt from their training and therefore understanding of AS2201.1. This required the placement of the intruder alarm system control panel within a protected area and to adequately protect the cables and devices of the system using single or dual end-of-line resistance supervision. As a sizable proportion of control panels currently in use are unable to support dual end-of-line resistance, AS2201 was analysed to establish compliance.

UNDERSTANDING SECURITY TECHNOLOGY

Learning and understanding the concepts associated with technology applied to the protection of assets can be considered at a range of levels, according to requirements for performance. The cognitive domain can be structured as a hierarchy of understanding of levels of security technology (Smith and Robinson, 1999, p. 28). One of the most universally applied models is the Taxonomy of Educational Objectives (Anderson, 1995). The study presents examples of how the Taxonomy may be applied to security installers. Accordingly, levels of understanding range from simple to complex, and from concrete to abstract in difficulty.

Bloom's revised taxonomy is based on a six level thinking process. It is suggested the first three levels apply to training within the security industry and the second three levels apply to education within the security industry. A proposed hierarchy of understanding for security technology can be presented as:

Remembering is the lowest form of the taxonomy and only requires recall or recognition of specific facts, universal principles, or methods. This elementary understanding of concepts only requires recall of fragmented knowledge of security technology without application; for example, the use of PIR or Quad sensors for the office area and Dual Tech sensors for the warehouse.

Understanding asks to explain something by making links to new ideas or concepts and requires the learner to explain and summarize chunks of information. The comprehension level of understanding of security technology allows the individual to describe the context of the detection system; for example, passive infrared detectors should not be installed facing into direct sunlight.

Applying requires making use of what is already known by applying knowledge in a practical way to both familiar and unfamiliar situations. An understanding at the application level will allow prediction of outcomes from a set of data or information; for example, calibrating and programming a PZT camera.

Analysing requires the deconstruction of information, ideas and concepts into parts so as to distinguish between sorts of information and categorization. The understanding through analysis of an idea is a higher level of abstraction and requires a detailed comprehension of function of the concept; for example, the probability of risk at each of the rings of defense in the protection of an asset.

Evaluating is a skill developed in thinking critically in order to be able to justify a decision or course of action. The ability to integrate two or more major ideas into a coherent and internally consistent principle to better understand a security technology system represents this level of understanding; for example, the integration of the protection-in-depth principle of asset protection with the crime prevention through environmental design (CPTED) strategy to synthesize a model that has both social awareness and target hardening features.

Creating is encouraged, for developing new products, ideas or novel ways to solve problems. This level of understanding of the principles governing the concepts of security technology requires both qualitative and quantitative judgments as seen with the introduction of wireless security technology (oz-teachernet, 1995; Smith and Robinson, 1999, p. 29).

PROTECTION OF ASSETS

Protection-in-depth (Garcia, 2001) or Defense-in-depth (Smith and Robinson, 1999; Smith, 2003) means that to accomplish the goal, an adversary should be required to avoid or defeat a number of protective devices in sequence. Often central to the protection of assets is an intruder alarm system. The core components of an intruder alarm system are the control panel and the inter-connected detection devices.

An intruder alarm system may be defined as a component or element of a physical protection system. The ultimate objective of a physical protection system is to prevent the accomplishment of overt or covert malevolent actions. Typical objectives are to prevent sabotage of critical equipment, theft of assets or information and protection of people. The physical protection system must accomplish its objectives by either deterrence or a combination of detection, delay and response (Garcia 2001, p. 54). Deterrence can be achieved through signage advising of the protection of premises by the intruder alarm system and by the prominent display of external warning devices, such as sirens and strobe lights.

Detection is the discovery of an adversary action and includes sensing of convert or overt actions. To discover such action, the following events need to occur:

1. A sensor reacts to a stimulus and initiates an alarm.

2. The information from the sensor is reported and displayed.

3. A person assesses the information, judges the alarm to be valid or invalid and initiates a response.

These events show that detection is not an instantaneous event. Included in the detection function of physical protection is entry control. Entry control allows entry to authorised personnel and detects the attempted entry of unauthorised personnel and material (Garcia 2001 p. 55). With an intruder alarm system, delay before detection is primarily a deterrent. Once detection has initiated the alarm system, the appropriate response may be to send a guard or advise the clientele. A monitored alarm system can report and display an intrusion within a very short time frame. Response time to electronic alarm systems is dependent on the proximity of the response personnel. The study concentrated on the element of detection.

THE SECURITY INDUSTRY

Security agents or their employees who provide or deliver contract security services are usually required to be licensed by police authorities. Licensing requirements involve police screening of individuals to ensure that they are 'fit and proper people' to provide security services; i.e., have no criminal record or known criminal associations. Licensing may also include examinations of basic technical knowledge, for example, knowledge of relevant Australian standards and legislation, appropriate qualifications, and annual checks of security business records (Tate, 1995, p. 29). Tate (1995) suggested that legislation covering the security industry did not necessarily specify the purpose or type of training.

Training content is decided variously in different states by Department of Consumer Affairs, Police Agencies and Technical and Further Education (TAFE) departments. A common requirement is that licensing courses satisfy legal requirements and are, in some way, accredited. Currently, license applicants usually need to demonstrate technical competence before a license is issued. Developing compulsory training according to accredited industry competency standards could facilitate standardization of respective state licensing requirements that, in turn, would enhance the mobility of security occupations. In the absence of an industry training framework and the consequent reliance on enterprise training, the security industry appears to have territorial attitude to training (Tate, 1995, p. 34).

The risk of an enterprise losing its investment in trained people to its competitors is real and causes a circumspect approach to training. The development of an industry training system will increase the pool of industry expertise, which utilise the risk of defection of valuable employees, foster a more open approach to training and create a more flexible workforce. Security industry training tends to be in the form of short technical courses to satisfy legislative requirements or to enhance existing technical skills. This approach exemplifies a work community sustained by mature age recruits who acquire vocational skills in other occupations and require bridging training for a security occupation. According to Tate (1995), this may partly explain why the industry seems to need a significant emphasis on high level behavioural skills rather than technical skills.

Security Installers

A survey of West Australian contract security enterprises provided the following information, supplemented with 1991 census information (Tate, 1995, p. 30). This functional structure of the security industry workforce was also suggested by Smith and Robinson (1999, p. 30).

Senior technicians were mainly employed by companies dealing with electronic equipment. They were regarded as highly skilled.

Technicians were most commonly employed in companies dealing with alarms, monitors, security doors and grilles, and fire detection services. They were regarded as being highly or adequately skilled. Most were required to have a police license.

Senior installers were mainly employed in small and medium-sized companies, primarily dealing with alarms and security doors. Two thirds were considered to be highly skilled; the reminder adequately skilled. They were required to have a police license. About half were required to have a TAFE qualification.

Installers were primarily employed by companies with less than twenty staff dealing in alarms, locks and security doors; the largest number employed by companies of five or less staff. They all require police licenses but very few needed TAFE qualifications.

Common practice within the industry is for those with trade qualifications to advance to the positions of technicians, while those with some form of training in the security industry advance to positions of installers. Currently, security systems installers are drafted either from other industries and cross-trained on the job or trained as apprentices by the major security companies. It is argued that the weakness in this system is that there is no security apprenticeship course that satisfies specified industry standards. Trainees enrol in the apprenticeship course modules approximating those required by the industry, for example, electrotechnology servicing, electronics, electrics and develop specific security skills on the job (Tate, 1995, pp. 36-37).

Given the size, scope and importance of the industry, the availability of training is very limited at all levels. Training is mainly in response to legislative and enterprise requirements, and based on a work force trained in other industries. On-the-job training is provided for unqualified intruder alarm system and security doors installers. Just-in-time technical training is supplied on-the-job for installation projects requiring new products or new technology, offered by the manufacturers. Major companies offer electronics servicing apprenticeships based on enterprise standards.

THE STUDY

A random survey (n=20), conducted by technicians (n=10) from one of the larger Perth security companies, analysed two aspects of the Australian Standards 2201.1 for installation of intruder alarm systems in both domestic and commercial premises within the Perth metropolitan area. The location of the intruder alarm control panel and the tamper monitoring resistance protection of its devices were measured. In combination, these two aspects of security installation should determine, to a degree, the ability of Perth security installers to install alarm systems to Australia Standard AS2201.1; "systems installed in a client's premises".

Under the principles of defense in depth, the control panel of an intruder alarm system should be located within the alarmed area and protected by one of its own detection devices. Upon activation, the sensor protecting the

control panel should trigger an instant alarm, that is, without delay. This detection method was the basis for questions one and two of the survey:

Question 1: Is the Control Panel or it's DGP's directly covered by an alarm detection device i.e. reed switch or PIR?

Question 2: Is the Control Panel or Data Gathering Panel (DGP) located in an entry/exit area?

Zone supervision
AS 2201.1: 1998 section 3.11 states for wired detection circuits:

> "Every wired detection circuit shall be a monitored circuit and shall generate an alarm condition on occurrence of any of the following events:
> 1. All short circuits and all open circuits.
> 2. Any series or parallel substitution of the end-of-line component by a component of value equal to that specified by the manufacturer" (p.15).
>
> Monitoring of a detection circuit through zone supervision is usually accomplished by a set resistance determined by the manufacturer of the control panel for each particular alarm system. Common resistance configurations are:
>
> *Single end-of-line* One resistor in series or parallel per zone.
> *Split end-of-line* Two resistors, one for each zone, used to zone double a control panel and increase its number of allowable zones from say 4 to 8, 6 to 12 or 8 to 16 by using appropriately sized resistors as specified by the manufacturer.
> *Dual end-of-line* Two resistors in series or parallel per zone.
>
> Single or split end-of-line resistors will satisfy clause 3.11 (a) only if the alarm system is armed. If disarmed, an open circuit or short circuit will show as a normal fault, for example, an open door or movement in front of a sensor. As for clause 3.11 (b), such substitutions are not always detected by single and split end-of-line systems.
>
> Dual end-of-line resistance however, is designed to detect open circuit, short circuit and resistor substitution whether the alarm system is turned on or not. Hence it is suggested that not all burglar alarm control panels being used comply with clause 3.11 of AS 2201.1: 1998 as being capable of dual end-of-line monitoring. Some control panels are capable of all configurations but are not always configured dual end-of-line, while other control panels are not capable of dual end-of-line resistance.

This section of the standard provided the basis of the third and fourth questions: *Question 3:* What is the form of zone supervision and *question 4:* Is the control panel capable of dual end-of-line resistance?

Questionnaires were distributed to intruder alarm system technicians (n=8) from a participating security company. The questionnaires were attached to randomly selected service and maintenance dockets for the Perth metropolitan area. The questionnaires were completed by the technicians during their normal course of business and returned to the supervisor each evening. Twenty completed surveys were returned by four of the technicians over the following week.

The collected data was transposed into an Excel sheet, listing the response to each of the four questions within the relevant postcode area. Postcodes in the Perth metropolitan area are designated as either north or south of the Swan River. Postcodes 60*xx* are determined north and postcodes 61*xx* are determined south. In this study, twelve sites were surveyed in the northern suburbs and eight sites surveyed in the southern suburbs. This data were evaluated and compared to the appropriate provisions in Australian Standard AS2201.1 and the Security and Related Activities (Control) Act 1996 for compliance.

ANALYSIS AND RESULTS

The survey data were analyzed, with interpretations resulting in a number of significant findings. These included the measure of compliance to AS2201.1 in the intruder alarm panel location, entry/exit location and zone

supervision. Finally, the findings allowed assumptions to be made regarding the current security industry, and system of legislation, licensing and training.

Question 1: Is the control panel directly covered by an alarm detection device?

Of the alarm systems surveyed, it was found that seventy percent of the control panels were directly covered by an alarm detection device. But thirty percent were not covered directly, providing greater opportunity for interference.

Question 2: Is the control panel located in an entry/exit area?

In eighty five percent of the alarm systems surveyed, the control panel was located outside the entry/exit area. Fifteen percent of the control panels were found to be located within this area, susceptible to easier attack.

Question 3: What is the form of zone supervision?

Forty percent of the alarm systems surveyed were operating under single resistor zone supervision. Sixty percent of the alarm systems used dual end-of-line resistance.

Question 4: Is the control panel capable of dual end of line resistance?

Of the alarm systems surveyed, seventy percent of the control panels were capable of dual end-of-line resistance. But thirty percent of the control panels did not have this capability.

It was found when analysing the answers to questions three and four in combination, that ten percent of the control panels capable of dual end-of-line supervision reverted to single end-of-line resistance. When analysing the answers to questions one and two in combination, only one alarm system (5%) was found to have its control panel located in an entry/exit area and not be directly covered by an alarm detection device.

INTERPRETATIONS

Australian Standard AS2201-Part 1, Section 2: Installation and location of control equipment, states that control equipment shall be located within the alarmed area (1998, p. 8). The alarmed area is that part of an area to which detection is afforded by an intruder alarm system (1998, p. 6). The study survey found six (30%) of the twenty alarms observed did not comply with this part of the standard.

Though not stated specifically, the control panel, under the principles of defense in depth, should not be located in an access route. This entry/exit area allows a set time for legitimate users to access the intruder alarm controlling equipment for arming and disarming. Personnel gaining unauthorized access to this area would be granted the same entry time as authorized personnel, creating a period of vulnerability for the alarm systems operating and controlling mechanism. Three (15%) of the twenty alarm systems visited had the main control panel within this access route.

The justification for assessing intruder alarm panel type was highlighted in the study. Some brands of control panel used in Western Australia and the Perth metropolitan area are only capable of using single end-of-line resistors for zone supervision. Three of the questionnaires answered *yes* to the capability of dual end of line resistance, where the panel type indicated (questions 4) were not capable of this supervision. As corrected on these questionnaires, six out of twenty systems checked did not have this capability and eight out of twenty systems were wired utilizing single end-of-line resistance. AS2201.1 indicates a monitored circuit (supervised circuit) is a circuit arranged to provide an alarm condition in the event of interference to, or failure of, the circuit (1998, p. 7). That tamper-detection devices should be included in the intruder alarm system and provide an appropriate warning signal while the alarm system is disarmed, should interference or failure of the circuit occur (1998, pp. 13-14).

In considering the study results, the following assumptions have been made:

1. A degree of current installers either do not comply or do not understand the applied Australian Standard 2201.1.

2. The security industry licensing regime is, to a degree, ineffective in providing the community compliant intruder alarm systems.

3. The security industry, through self regulation, appears to be ineffective in maintaining compliance. 4. Additional education, training or awareness needs to be applied to the installer group to raise compliance standards. This supports Tate's (1995) comments on the lack of structured training within the security industry.

The study has provided an insight into the quality of intruder alarm system installation, which appears to be lacking. Although the study was relatively small, a larger statistically significant study will be completed. The mathematical formula proposed by Morrison, 1993, p. 117 indicates the appropriate size of a random sample for a population in excess of one million people; N=384 (Cohen et al, 2005, p. 94). This larger study will ensure that a reliably and valid understanding on the compliance of AS2202.1 will be gained.

SUMMARY

The study highlighted a number of significant points of interest. The first, that a percentage of intruder alarm systems inspected failed to comply with the standard set by AS2201.1 on two aspects; that of panel location (30%) and entry/exit location (15%) could be classed as higher than acceptable within the industry. Second, that the distribution and use within the security industry of intruder alarm panels that do not have the capability of dual end-of-line supervision (30%), as required by AS2201.1. Assumptions have suggested that the level of non-compliance is due to a lack of industry focused vocational training, that the security industry cannot provide an appropriate level of self regulation and therefore supervision. The current licensing regime is to a degree ineffective in testing entry requirements and finally, legislation is lagging behind the industry. No single aspect could be considered ineffective; rather it is argued that all these areas need to be addressed.

The combination of the Security Act and the Australia Standards for intruder alarm systems installed in client's premises provides specific regulation for the installation of such intruder alarm systems in Western Australia. With the increased importance of security, comes the importance of having an intruder alarm system installed to the standard. The study has shown that there are significant questions to be answered on intruder alarm system installation compliance. It is proposed a larger study will confirm the outcome of this study.

REFERENCES

Anderson, L. (1995). *Revised Bloom's Taxonomy*. Retrieved December 1st, 2005 from http://rite.ed.qut.edu.au/oz-teachernet/index.php?module=ContentExpress&func=display&ceid=29

Australian Standard 2201.1 (1998). *Intruder Alarm Systems. Part 1: Systems Installed in Client's Premises.* Homebush: Standards Australia.

Cohen, L., Manion, L., & Morrison, K. (2005). *Research Methods in Education* (5th ed.). New York: RoutledgeFalmer.

Department of Education and Training. (2006). *TAFEWA: Discover your future*, from

http://psc.tafe.wa.edu.au/TAFEWACourseSearch/CourseDetails.aspx?lookup=&CID=WS83&AKEY=1176433&title=Electrotechnology%20Servicing%20(Security%20Systems)&CollegeID=13

Garcia, M. L. (2001). *The Design and Evaluation of Physical Protection Systems*. Burlington: Butterworth-Heinemann.

Green, G., Edwards, K., & Netolicky, D. (2002). *Bloom's Taxonomy*. Retrieved November, 2005 from (CD) Published by Presbyterian Ladies College - Cottesloe

Hemmens, C., Maahs, J., Scarborough, K. E. & Collins, P. A. (2001). Watching the watchmen: State regulation of private security 1983-1998. *Security Journal*, *14*(4), 17-28.

Keller, S. and Chuvala J. (1992). Training: Tricks of the trade. *Security Management 36(7)* 101-105.

Oz-Teachernet. (1995). *Revised Bloom's Taxonomy*. Retrieved December 1, 2005 from http://rite.ed.qut.edu.au/oz-teachernet/index.php?module=ContentExpress&func=display&ceid=29

Prenzler, T. (2005). Mapping the Australian Security Industry. *Security Journal, 18*(4), 51-64.

Security and Related Activities (Control) Act 1996. Reprinted (2003). Perth: Government Printers.

Smith, C. L. (2003). *Understanding concepts in the Defense in Depth Strategy.* Paper presented at the Proceedings of the 2003 International Carnahan Conference on Security Technology. pp. 8-16.

Smith, C. L., & Robinson, M. (1999). *The Understanding of Security Technology and its Applications.* Paper presented at the Proceeding of the 1999 International Carnahan Conference on Security Technology. pp. 26-37.

Tate, P. W. (1995). *Report on Security Industry Training: Case study of an emerging industry*. Perth: Western Australian Department of Training. Western Australian Government Publishing.

COPYRIGHT
Robert E. McLaughlin and David J Brooks ©2006. The authors assign SCISSEC & Edith Cowan University a non-exclusive license to use this document for the personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites of the World Wide Web. Any other usage is prohibited without the express permission of the authors.