Proceedings of the 12th Colloquium for Information Systems Security Education
University of Texas, Dallas
Dallas, TX June 2 - 4, 2008

# Information Assurance Education In A Specialist Defence Environment

Les Smith, Emeritus Prof William Caelli, *Queensland University of Technology*, and Neil McNair, *No. 462 Squadron-RAAF*

**Abstract** – ***The RAAF's imperative is to train members of its No 462squadron in the appropriate disciplines required for the squadron to meet its charter. As a result No 462 Squadron and the Queensland University of Technology, in Brisbane, Queensland, Australia have developed a prototype training and education program designed to meet the Squadrons charter in a cooperative effort between a defence establishment and a public academic institution.***

***This paper discusses the experience gained in the development and delivery of a formally recognised Australian tertiary qualification in information assurance designed to meet No 462 Squadron's Information and Communications Technology (ICT) and Information Assurance education and training requirements.***

## I. INTRODUCTION

Early in the last decade the Royal Australian Air Force (RAAF) introduced limited numbers of stand alone Personal Computers (PC) across the organization. By mid decade, RAAF commenced roll out of a national protected Wide Area Network (WAN) connecting that entire group of stand alone PCs previously installed. As the WAN continued to develop RAAF identified a parallel increase in the need for Information Security (INFOSEC) practitioners. By 1997, RAAF had established a number of civilian ICT (Information and Communications Technology) employees within its Directorate of Security and Policing (DSP-AF). The primary responsibility assigned to these civilians was established to be in line with standard commercial IT security practices of the time.

At the same time senior RAAF executives decided upon an advanced program for the further development of Air Force capability in the emerging military area of Information Warfare or Info Operations (Info Ops). To this end the Air Commander Australia (ACAUST) proposed the synthesis, integration and coordination of existing technical security roles and functions already present within the RAAF.

The ACAUST proposal was endorsed by the RAAF and an operational directive was issued creating the RAAF Information Operations Squadron (IOSQN) with effect 31 March 2001. IOSQN was officially renamed *"462 Squadron"* with effect April 2005.[i]

## II. SQUADRON HISTORY

No. 462 Squadron, Royal Australian Air Force was formed at Fayid, Egypt, on 6 September 1942. The squadron joined the UK's Royal Air Force (RAF) Middle East Command and, operating Halifax heavy bombers, conducted operations throughout that theatre in World War II. In January 1943 the squadron relocated to Solluch in Libya and its main role became the conduct of attacks on harbours and shipping in Sicily. It moved again in February that year to Gardabia in Tunisia to operate in support of the ground campaign there, returning to Libya when these operations drew to a close in late May 1943. Operating from a succession of airfields in Libya – Hose Raui (22 May – 1 October 1943), Terria (1 October 1943 – 1 January 1944), and El Adem (1 January 1944 – 1 March 1944) – the squadron resumed operations over southern Europe, striking at targets in Italy, Sicily, Greece, Crete and the Dodecanese Islands.

The squadron relocated to Foulsham England on 29 December 1944 and joined "*100 Group"*, a specialist formation tasked with disrupting the German air defence system through the employment of diversionary raids and various radio countermeasures. The squadron's operations played a critical role in drawing German attention away from real raids. It continued in this role until its last operation was flown on the night of 2 – 3 May 1945.

This role and function was to become highly relevant in its new manifestation. After the end of the war in Europe, 462 Squadron continued training and was also employed in a transport role, which included the repatriation of Allied prisoners from Europe. It disbanded on 24 September 1945.[ii]

### 2.1 462 SQUADRON TODAY

No 462 Squadron is one of a number of units which make up the Information Warfare Wing of the Royal Australian Air Force's Aerospace Operational Support Group. The Squadron's mission statement is

> *"To enhance and protect RAAF combat capability through the provision of comprehensive, timely and integrated Information Operations."*[iii]

The Squadron is heavily reliant on specialist facilities, relevant equipment and highly-skilled people who have expertise in a wide range of disciplines comprising, specialist engineers and technicians, computer system operators, skilled and experienced analysts, project and capability management staff and logistics specialists.

### *2.2 Changing Cohort*

Effective multi-skilling can act as a force multiplier for smaller organisations. Like the other services that, together with the Royal Australian Air Force, make up the Australian Defence Force (approximately 55,000 serving personnel as at 2008 against a total Australian populations of around 21 million people[iv]) the RAAF has a great tradition of multi-skilling in both the enlisted and civilian sectors of the service.

The civilian positions originally established to support the RAAF DSP-AF have been incorporated into the new Squadron and combined with military personnel to develop new defensive capabilities. Although the new cohort exhibited widely diverse backgrounds and experience, further training and education in Information and Communications Technology (ICT) as well as in Information Security / Assurance was seen as an urgent need

### *2.4 RAAF Imperative*

With multiple new staff requiring enhanced IT security/assurance skills the RAAF's reliance on non-defence department based training and education providers continued with a proportional increase in expenditure required.

As development of new IT roles progressed within 462SQN, skill requirements for personnel evolved to a point where most commercially available IT courses were not entirely suitable. As most standard "off the shelf" training would include one or two required elements, Squadron personnel needed to be enrolled in multiple courses to gain all necessary skills. At the outset a "shotgun" type of approach was used for course selection with lots of people being sent to lots of courses.

This approach provided some capability within the Unit but was fiscally inefficient. The course selection process evolved into a "cherry picking" activity in an effort to target required skills. While this was more efficient it still lacked the precision required.[1] Whilst there was a need for specialist training there was also a need to educate squadron personnel in the day to day requirements of general matters in overall Information Assurance.

Shortly after the formation of the IO Squadron in 2001, one of the authors of this paper, Prof W. Caelli from Queensland University of Technology (QUT), gave a presentation on IO and Information Assurance to the squadron with an exposure to the themes being developed by then USA National Colloquium for Information Systems Security Education (NCISSE). As a result it was decided to approach Prof Caelli and QUT's then "Information Security Research Centre (ISRC), now subsumed into the Information Security Institute (ISI) at QUT, to see if the university could assist with the Squadrons education and training requirements. Prior experience based around the USA's NSTISSI 4000, now the under the auspices of the "Committee on National Security Systems" (CNSS), series of curriculae / instructions from the USA were also considered along with a review of experience in such education and training in other countries of relevance.

## III. QUT

Based in Brisbane, Queensland, Australia, QUT is considered to be a university which has a reputation for quality undergraduate and post graduate courses with a "real world" emphasis. It offers a wide range of studies and research activities best suited to meeting the needs of industry, the professions and the community.

QUT's Information Security Institute (ISI) is a multi-disciplinary institute that specialising in the development of information security and assurance solutions for government, business and the community by undertaking

[1] It is acknowledged that at that time no consolidated information security curriculum existed as an overriding requirement specification for use within the Australian Defence establishments.

research in technological, legal, policy and governance issues related to information security.

## IV. COURSE DEVELOPMENT

### *4.1. Adapting Prior Education Schemes and Practices to Meet Squadron Needs*

A *"Graduate Certificate"* program at QUT, delivered in intensive mode, was seen to fit the squadron's needs for this prototyping effort in that it provided both the diverse education experience required by the Squadron as well as being formally recognised as an Australian approved tertiary qualification. In this way Squadron personnel would be enabled to work further toward more advanced qualifications at the Post Graduate Diploma or Masters Degree level.

However, both QUT and the squadron recognised the need for appropriate professional industry level certification processes to be available to successful participants in this program. As mentioned above, a proposed curriculum based round that already developed and set out by the United States' *"Committee on National Security Systems (CNSS)"* [v], formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC). Given the need to consider the multi-skilling requirements of the Squadron, allied concepts in education and training set out by the *"International Information Systems Security Certification Consortium (ISC)$^2$"* (CISSP) and by *"ISACA"* (CISM) programs were considered in development of a "best fit" option. This decision to consider the bases for differing but yet complementary industry oriented education and training programs was an important development since the cohort involved in this specific educational program could be readily separated into two distinct streams, viz. those interested and experienced in a managerial/policy oriented stream and another in a technology/engineering stream. At the same time, and in distinct contrast to many other programs of study, the educational background of the cohort was diverse in both discipline areas and level of formal education and training. This factor alone came as a major contrast to many other programs in defence establishments where a finer control of entry requirements for such a course could be maintained.

A review of existing courses and course materials / pedagogic processes offered through QUT's normal or standard post graduate program in ICT quickly established that much of the course material available was not suitable for the particular task the university was being asked to undertake. Whilst it was essential that course content did not contain nationally classified material or processes, much of the course material finally selected and used was considered to be sensitive in nature in relation to both the materials presented and the circumstances of such presentation. This included carefully selected case studies. Thus a general agreement was reached that for citation purposes the *"Chatham House Rule"* would apply. This rule, dating from 1927, is as follows:

*"When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed".*

As stated on its relevant website[vi]:

*"The world-famous Chatham House Rule may be invoked at meetings to encourage openness and the sharing of information."*

### *4.2. Adoption of ISC$^2$ Course Concepts*

It was now decided to develop additional new course material which was purposed designed. The original overall education program concept called for the offering of three *"units"*, the QUT term used to describe an individual module of study, related directly to ICT Security and Assurance and then a fourth unit designed around the topic of *"computer forensics"*. Elsewhere this module may be known as a *"course"* or *"subject"*. In normal academic mode, a *"unit"* of study at QUT consists of approximately 40 hours of class contact including formal lecture and/or tutorial sessions. In base terms, four such units comprise a *"course"*, elsewhere sometimes referred to as a *"program"*. For example, a *"Graduate Certificate"* at QUT is granted on the successful completion of such a course consisting of four units of study. A "Graduate Diploma" entails successful completion of 8 such units and a "Masters" degree, 12 such units, although 4 units may be joined into a single activity such as preparation of a minor thesis, suitable project, etc.

Additional time in laboratory sessions or using Internet based educational materials may be added to this. After some consideration it was decided that the overall topic of computer forensics organised into a single and separate module would be to complex to deliver effectively over a five (5) day intensive class contact period. It was thus decided to incorporate forensics concerns and materials into individual modules as appropriate, gradually increasing the forensics content in each particular case, e.g. network authentication technologies, etc. over the entire course.

The pedogical processes required in course delivery, given that the cohort consisted of members with at least

some years of post high school defence experience and could be regarded as being "mature age" entrants, required that different approach be developed for day to day course operation. Members of the ISI would be coopted to develop and deliver specialist course content as required.

The first module was designed to be an *"Introduction to Information Security"* and was loosely based upon Chapters 2 – 12 of the *"All in One CISSP Exam Guide"*[vii], which was chosen as the course textbook. This has since become the foundation module of the training program and is taken by all members of the squadron. It was also considered that this approach would provide course participants with the necessary knowledge to undertake the ISC$^2$ CISSP certification process if they so wished.

*4.3. Daily Routine*

After considerable experimentation and given that units were being presented in an intensive mode over a period of usually five contiguous days involving full-time eight-hour participation of the student per day, the following daily pattern emerged as the most acceptable and successful format for all modules delivered. One exception involved the decision to run a *"Boot Camp Day"* in Module One, the *"Introduction to Information Security"* unit. Daily sessions were established as follows, with five "sessions" before lunch and four after the lunch break:

- Session one, was a review of the days learning outcomes and associated program together with a review of any outstanding logistics or learning concerns.
- Session two, three, four and five consisted of traditional lectures and allied material presentations together with associated class feed back.
- Sessions six and seven, normally after lunch, involved individual assignments based upon materials presented and discussed in the previous four sessions.
- Session eight saw the presentation of any additional material, revision and re enforcement.
- Session nine was a question and answers group discussion session together with a review of any overnight study or assignment activities.

This became the normal daily format which emerged through practical experience in relation to class dynamics and student needs.

*4.4. . Boot Camp*

This specific day was broken into the following segments. Segment 1 - expectations of learning outcomes for the day followed by details of the daily program;
Sessions 2 and 3 were based on the expectation that the cohort would be broken into two parallel streams designated as separate sessions entitled *"Policy for Technology Professionals"* and *"Technology for Policy Professionals"*.[2] The remaining sessions followed the normal daily format following the structure detailed in paragraph 4.3.

*4.5. Findings*

A major finding of this program was that given the specifics of this defence personnel cohort it was essential to divide the lecture / presentation sessions into no more than 40 to 45 minute periods with 15 minute breaks. As these courses are delivered on a defence site, there has been a tendency for course participants to return to their work place during breaks. Therefore, it is essential to enforce strict adherence to the time table.

After three iterations of the overall program, the following factors for successful program operation in this environment have been found:

**Factor 1** - flexibility in course content and presentation methodology is essential for an unpredictable and diverse defence cohort intake.

**Factor 2** – there must be room in the program to enable necessary background educational processes to occur. This was demonstrated through the success of the *"Boot Camp"* activity in the third iteration of Module 1.

**Factor 3** - program presenters need to be comfortable with the fact that not all course activity will be successful and must be capable of working around and compensating for perceived failures when they occur.

**Factor four** - learning styles may differ radically across perceived groupings in the overall cohort. For example it became clear that learning methods for technically oriented defence

[2] In the 3rd delivery of this module these two streams were combined due to limitations in student numbers.

personnel could be quite different to those with managerial, legal or policy functions.

**Factor five** - arrangements for appropriate assessment is required involving allowance for such factors as time, location and form of assessment as well as appropriate assessment supervision.

**Factor 6** - unique deployment imperatives specific to Defence operations must be considered when planning for both presentation and assessment activities.

The graduate certificate program, from the experience gained, finally settled into the following structure involving a total of 160 hours of formal class contact or its equivalent:

- Week 1: Introduction & Risk assessment
- Week 2: Network Security
- Week 3: Systems & Application Security
- Week 4 (Equivalent minimum time expenditure): Individual Project

It should be noted that the project activity, when used, involved the definition and agreement to both topic and project work duration. In addition, agreement as to the type and nature of the assignment project had to be vetted by both the university and the squadron, e.g. the project and its final report had to involve work not subject to national security classification.

## V. CONCLUSION

The most likely evolution of training development for No 462 Squadron will be to analyse personnel capabilities and competency down to the individual operational level and then clearly articulating those competencies required for each functional element of this defence Unit. By articulating competencies required the Squadron should be able to release tenders or requests for price quotations for training services from entities able to provide the skills necessary to deliver required outputs. Efficiencies gained by focusing training delivery to required competencies should result in better use of capitol effectively increasing funds available for staff development.

An ancillary but important consideration is motivation and job satisfaction for Squadron personnel. The Squadron aims at development of a professional, cohesive and confident workforce by providing an opportunity to gain a nationally recognised tertiary qualification.

Placement of particular emphasise on defence, national and international standards and processes was agreed to be an important of the overall education process, including those not specifically related to information security or assurance but considered to be of significance. Specifically the Australian Defence Department's *"ADFP 102 Defence Writing Standard"*, was adopted for all written materials to be developed and presented by the students. After serious research, as mentioned above, it was also decided to adopt the *"All in One CISSP Exam Guide"* as the base text. This was combined with the ISO / ANZS 17799/2700 series of *"Information Security Management"* standards[viii], the AS/NZ 4360 *"Risk Management"* standard, the Australian Government Information and Communications Technology Security Manual ACSI 33[ix], and, where appropriate, United States Government NIST FIPS publications were selected and used including, FIPS-199/200[x].

## REFERENCES

[i] Neil McNair *"Data Fusion Tools For Small Deployed Operations"* 2005 - Phoenix Challenge Conference - Spring 2006 Johns Hopkins University Applied Physics Laboratory, Baltimore, MD, USA

[ii] Australian War Memorial – History of No 462 Squadron RAAF www.awm.gov.au/units/unit_11167.asp

[iii] No. 462 Squadron's Mission Statement

[iv] Australia's population projection to 9 March 2008 by the Australian Bureau of Statistics (ABS), cited at URL http://www.abs.gov.au

[v] URL for CNSS cited at 9 March 2008 is http://www.cnss.gov

[vi] URL at 9 March 2008 is http://www.chathamhouse.org.uk/about/chathamhouserule/

[vii] Shon Harris – All in One CISSP Exam Guid3McGraw-Hill/Osborne – Third Edition ISBN 0-07225712-1

[viii] URL cited at 9 March is http://www.standards.org.au/

[ix] URL cited at 9 March 2008 is http://www.dsd.gov.au/library/infosec/acsi33.html

[x] URL cited at 9 March 2008 is http://csrc.nist.gov/publications/PubsFIPS.html