December 2003

Australian Forensic Computing Investigation Teams: Research on Competence

Mathew Hannan
University of Tasmania

Paul Turner
University of Tasmania

Australian Forensic Computing Investigation Teams: Research on Competence

Mathew Hannan and Dr Paul Turner

School of Information Systems

University of Tasmania, Australia

Abstract

The risk of criminal, illegal or inappropriate computer behaviour continues to rise as information and communication technologies including the Internet become more pervasive globally. For many public and private sector organizations one response to managing these risks has been to establish Forensic Computing Investigation (FCI) teams. However, the dynamic and multi-disciplinary nature of the forensic computing domain means that decisions concerning the nature, level and type of competences that these teams should contain remains a challenge.

This paper presents research on competence among 21 Australian FCI teams and generates insights on anticipated key competences required to address the forensic computing challenges of the immediate future of computer misuse. Significant outcomes of this research include the identification of a core set of competences that currently exist amongst Australian FCI teams and the nature and type of skills' acquisition deployed.

Keywords

Competence. Forensic Computing. E-Crime. E-Forensics. Security. Learning and Development. Dynamic Technological Environments. Competence Measurement.

Introduction

The widespread diffusion of information and communication technologies including the Internet has given rise not just to new opportunities but also to new risks. In recent years the increasing risks of computer misuse have too often become a reality as individuals and/or groups have used new technologies to engage in criminal, illegal or inappropriate behaviour (ACPR 2000).

As with more traditional forms of social transgression, a variety of methods are available to address criminal, illegal or inappropriate computer behaviour. These include deterrence, education and security precautions. However, when computer misuse occurs it is often critical to conduct a formal investigation to: (a.) determine the effects of the misuse, and (b.) collect and analyse evidence to support future action. These actions may include criminal or civil prosecution, organisational censure or dismissal. Clearly, the conduct of these 'computer

forensic' investigations requires a range of specialised human skills that are increasingly in demand because of the increasing risk of computer misuse. Consequently, many public and private sector organisations have established forensic computer investigation (FCI) teams.

To ensure competent and comprehensive investigation, FCI teams require a multi-disciplinary mix of skills to enable them to deal with the variety of *post facto* investigations potentially criminal, illegal or inappropriate conduct committed by the use of, or involving, a computer or electronic device (Broucek & Turner 2001). However, the dynamic and multi-disciplinary nature of the forensic computing domain means that decisions concerning the nature, level and type of competences that these teams should contain remains a challenge.

In the Australian context, this paper reports on initial research that has established a body of knowledge relating to Australian FCI team competence. This research contributes to filling a gap in existing knowledge relating to the competence contained within current FCI teams in Australia and generates perspectives on how these skill sets are evolving (Broucek & Turner 2001; Etter 2001a). It is anticipated that this body of knowledge will provide a basis upon which further research may be conducted within this field.

Theoretical Background

In developing a theoretical base for the research instrument that was deployed to measure team competence among Australian FCI teams, three key bodies of knowledge were examined. There were as follows:

- The measurement of competence and team competence
- Teams within rapidly changing technological environments
- The emerging discipline of Forensic Computing

Competence

For a number of years, researchers have attempted to identify the foundations of effective individual performance within a work environment. Initially some of this research focused on identifying the necessary skills required to undertake a job by observing employees at work in order to construct skill sets to formulate job requirements. Subsequently, McClelland suggested a link between the job and the knowledge, skills, abilities, traits or motives held by the individual (McClelland 1973; Schippmann et al. 2000). Then, Richard Boyatzis' (1982), building on the work of McClelland (1973), stimulated the use of the term "competency" as it relates to human resources within an employment environment (Woodruffe 1991) by defining it as follows:

> *(an) underlying characteristic of a person in that it may be a motive, trait, aspect of one's self-image or social role, or a body of knowledge which he or she uses (Boyatzis 1982:12).*

Since these early approaches, the notion of competence has been explored from the perspectives of a number of different disciplines including psychology, management, human resources management, education and information systems (Bassellier et al. 2001). Each of the disciplines tends to define "competence" in slightly different ways. Furthermore, different definitions exist within each discipline. Some of them make "competence" and "competency" synonymous with one another, which has led to differing connotations within

the literature (Woodruffe 1991; Hearn et al. 1996). Schippmann et al. (2000) even suggest that the word "competencies" today is a term that has no meaning apart from the particular definition with whom one is speaking" (Schippmann 2000:706).

It can be observed at a conceptual level regardless of the discipline, "competence" does possess generic attributes. These core attributes refer to human characteristics or knowledge that may contribute to or enable effective performance (Boyatzis 1982; Murlis & Fitt 1991; Dalton 1997; McLagan 1997; Dubois 2000; Schippmann et al. 2000; Bassellier el at. 2001). In this sense, regardless of the disciplinary definition, "competence" is independent of a type of technology, position, organisation, or industry (Bassellier et al. 2001).

In relation to teams, Prahalad and Hamel (1990) were the first to explore the notion of competence as more than individual attributes. Prahalad and Hamel suggesting that an organisation could possess knowledge, skills, abilities and other characteristics that provide the basis for an organisation's ability for rapid change and innovation (Prahalad & Hamel 1990; Schippmann et al. 2000). Prahalad and Hamel (1990) suggested that competence forms the roots of organisational competitive advantage and defined core competence as, "the collective learning in the organisation", (Prahalad & Hamel, 1990:82). They also suggested that it was possible to identify and mobilise core competence within an organisation and to develop long-term competitive advantage and above average returns (Prahalad & Hamel 1990; Hitt et al. 1997).

Therefore, the identification of core competence is possible through the examination of an organisation's core functions (Prahalad & Hamel 1990; Ward & Griffiths 1996; Hitt et al. 1997; Drucker & Gumpert 2000). The identification of an organisation's core competence is usually a function of senior management as a component of strategy formulation (Hitt et al. 1997).

The connection between organisational level core competence and individual competence is the knowledge acquired by the organisation or individual. The link can be observed within these definitions of competence as knowledge:

> *the collective learning in the organisation* (Prahalad & Hamel 1990:82)
>
> *a body of knowledge which he or she [the person] uses (Boyatzis 1982:21).*

Knowledge as a competence has arisen directly because of the complexity of the modern business environment and the influence of technology upon business practice (Bassellier et al. 2001; Epstein 2002). Competence as knowledge implies that the employee has a broader awareness of the task that extends beyond task specific competence (McLagan 1997; Bassellier et al. 2001; Epstein & Hundert 2002). The idea that knowledge be regarded as a competence is further supported by recent works of Hearn et al. (1996), Bassellier et al. (2001) Epstein (2002) and McLagan (1997).

The behavioural approach to competence measurement is centred on identifying the kind of competence that underpins successful performance and producing a generic list of relevant competence. Further, this method allows for separate measurements of competence and performance, thereby enabling the researcher to more closely examine the body of knowledge held by FCI teams within Australia.

Teams operating within rapidly changing and developing technological environments

One of the most difficult and important challenges faced by many modern organisations is the need to respond to seemingly ceaseless rapid technological changes (Henderson 1992). Hitt et al. (1997) suggest that technology has resulted in changing the base of organisational competitive advantage for superior performance. This change has resulted in the move from the traditional tangible resource base to less tangible organisational resources such as the knowledge possessed by employees (Ward & Griffiths 1996; Hitt et al. 1997; Robson 1997).

FCI teams operate in environments characterised by rapidly changing and developing technologies. The core to superior performance within these environments is in the development of knowledge. Knowledge is developed through both informal and formal experience including training. At an organisational level, this can be promoted through fostering an environment that encourages the acquisition of knowledge. The concept of knowledge as the key to superior performance among teams operating in rapidly changing technological environments forms the basis upon which to measure competence within FCI teams operating in Australia.

Forensic Computing

With the penetration of information technology into almost every facet of the Australian community has come the increased risk of the misuse of information, technology or electronic criminal activity (McKemmish 1999; ACPR 2000; ACPR 2001; Broucek & Turner 2001).

Within Australia there is a lack of comprehensive data that clearly identifies the level and incidence of electronic crime (ACPR 2000). Etter (2001) identifies non-reporting and non-detection of electronic crime as a significant factor for the absence of this data within Australia (Etter 2001b).

Several authors (Drucker & Gumpert 2000; Broucek & Turner 2001; Etter 2001a) suggest that the rapid development and increased uptake of technology within society has occurred more quickly than the development of a legal framework that is required to manage criminal, illegal or inappropriate conduct occurring within this medium. This has vast implications for Forensic Computing Investigators developing and maintaining legal knowledge relevant to their discipline.

The purpose of Forensic Computing is to mount a *post mortem* investigations into criminal or other inappropriate conduct committed by the use of, or involving, a computer or electronic device (Broucek & Turner 2001). Bates (1997) warns that the rules of evidence apply equally to Forensic Computing as they do to other types of forensic evidence such as DNA typing and fingerprint identification (Bates 1997). McKemmish (1999) supports this stance identifying that outcomes of Forensic Computing Investigations must involve a requirement for the evidence gained in the investigation to be of a level specifically related to the team's constructed purpose and be legally acceptable (McKemmish 1999).

McKemmish (1999:1) proposes the following definition for Forensic Computing

> *Numerous definitions for Forensic Computing have developed over recent years. The process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable*

McKemmish (1999) further proposes that Forensic Computing is comprised of four key elements:

1. The identification of digital evidence
2. The preservation of digital evidence
3. The analysis of digital evidence
4. The presentation of digital evidence

Within these four elements, McKemmish (1999) recognises the importance of knowledge possessed by the investigator or investigating team that is broader than technical knowledge. He also identifies that these skills may require a high level of proficiency requiring specialisation.

Broucek and Turner (2001) further developed the concept of Forensic Computing as a multi-disciplinary academic field with reference to McKemmish's definition, and citing the work of other authors including Farmer (2001) and Venema (2000). They argue that in the absence of an overarching taxonomy, Forensic Computing research has failed to combine and leverage the strengths of individual disciplinary investigations of particular forensic issues. To overcome this, they proposed a taxonomy for the discipline that includes multiple dimensions and sub-categories upon which to frame the future development of the discipline. Table 1 provides the expanded dimensions within the proposed taxonomy.

Computer Science
• Operating Systems and Application Software
• Computer Security
• Systems Programming and Programming Languages
Law
• Computer Law
• Criminal, Civil and Technology Law (CCT Law)
Information Systems
• Systems Management and Policies
• User Education
Social Science

(Adapted from: Broucek & Turner 2001)

Table 1 Proposed Taxonomy: Forensic Computing

Broucek and Turner's (2001) taxonomy was used as the basis for the development of the instrument for the measurement of FCI team competence within this research study.

Within this research the term **Forensic Computing Investigation** is defined as:

> *Investigation into criminal or other inappropriate conduct committed by the use of, or involving, a computer or electronic device.*

Methodology

This research was undertaken using a positivist epistemology (Neuman 2000; Babbie 2001). Quantitative data was collected via the use of a questionnaire instrument. This instrument enabled analysis and a degree of generalisation of findings (Neuman 2000; Babbie 2001). The questionnaire was administered 30 Forensic Computing Investigation team leaders within Australia. Descriptive and inferential analyses were undertaken on the data obtained from the completed questionnaires.

The absence of a pre-developed instrument necessitated the development of a new instrument to undertake this study. A questionnaire was specifically developed for this research through the adaptation of traditional competence measurement techniques to assess team competence in a rapidly changing technological environment. The questionnaire was further designed to obtain data upon which analysis could be undertaken to meet the purpose and objectives of this research. Forensic Computing Investigation team leaders in organisations currently conducting FCI in Australia completed the questionnaire.

Broucek and Turner's (2001) taxonomy was used as the basis for the development of the instrument for the measurement of FCI team competence within this research study. The academic disciplines were used to provide the areas of competence to be measured within the FCI teams.

The questionnaire consisted of 22 questions divided over three parts, all relevant and specifically related to the objectives of the research. The three parts were:

- Demographics
- Competence of Team
- Desirable Competence

Questions were selected and developed in order to provide data upon which statistical analysis could be undertaken that directly related to the purpose of this research.

Email was selected as the most appropriate method of delivery for the questionnaire, based upon the potential participants' preference for the use of email.

At the commencement of this research, a comprehensive list of all organisations currently conducting Forensic Computing Investigation within Australia did not exist, rendering the construction of a population for this study impossible. It was therefore necessary, as outlined in Section 3.11, to develop a sample - that included as comprehensive as possible- a list of organisations currently engaged in Forensic Computing Investigation within Australia.

The identification of such organisations took place predominantly through consultation with people currently engaged in Forensic Computing Investigation, and liaison with industry bodies including Action Group for Law Enforcement of the Electronic Community (AGEEC), Australasian Prudential Regulatory Authority (APRA), and the Australasian Computer Crime Manager's Group.

Further sources such as research through the Internet and literature, were also used to develop the sample.

An exhaustive list of 30 organisations compiled by the researcher, included representative organisations from law enforcement agencies, accounting firms, government organisations, insurance organisations, federal regulatory bodies, commercial transport providers and other industry segments. The questionnaire was delivered via email to the recipients via group email on the 23 September 2002 (recipient list suppressed).

Reliability and Validity

Questionnaire research is generally considered weak on validity and strong on reliability (Babbie 2001). In the context of a questionnaire, validity refers to how the instrument adequately measures what it was designed to measure (Babbie 2001). In order to improve the validity of this research, a number of measures were taken to improve the accuracy of the data collected during the design of the questionnaire.

Throughout the development of the questionnaire face validity, criterion-related validity, content validity, and construct validity were taken into account to maximise the overall validity of the survey.

- The questionnaire addressed **Face validity** through the provision of operational definitions to clarify the meaning of terminology, in order to prevent misunderstanding by the participant
- **Content validity** was maximised through measurement across the range of meanings or definitions as contained within competence areas of Forensic Computing Investigation teams
- **Construct validity** was considered throughout the design of the questionnaire to allow appropriate measurement of variables to enable meaningful analysis

Questionnaire Construct

The questionnaire consisted of 22 questions divided over three parts, all relevant and specifically related to the objectives of the research. The three parts were:

- Demographics: This section of the questionnaire contained 13 questions designed to gain data upon which further analysis could be conducted relating to demographic information.
- Competence of Team: Part two of the questionnaire consisted of six questions specifically addressing the current competence held by the Forensic Computing Investigation team and how this competence had been developed.
- Desirable Competence: Part 3 of the questionnaire was designed to gather information relating to what Forensic Computing Investigation team leaders believe to be the most important to Forensic Computing Investigation now and into the future and the most desirable methods of developing competence

Questions were selected and developed in order to provide data upon which statistical analysis could be undertaken that directly related to the purpose of this research. The questionnaire was developed to include questions suitable for administration to a supervisor, team leader, Sergeant or Inspector (or equivalent rank) leading a Forensic Computing Investigation Team (or being the sole Investigator within an organisation). Part 2 and Part 3 of the questionnaire were predominantly developed using the proposed taxonomy of Broucek and Turner (2001) using a combination of nominal, ordinal and scale based questions to obtain data in suitable form for analysis.

The Impact of Small Population

Many widely accepted statistical analysis techniques have been developed for use by researchers dealing with small samples through to large and almost infinite population sizes (O'Rourke 2000). This contrasts greatly with this research study as this study features a large representation from a small population (30 identified Forensic Computing Investigation teams).

Statistical sampling is based upon the premise that, even if a small number of units are randomly selected from a much larger population, the characteristics identified in the small population will reflect the sample characteristics in the larger population (O'Rourke 2000). This represents the basis for more traditional quantitative statistical-based research. However, this research project differs from more common quantitative studies because of the following characteristics:

- Small sample size
- Large sample relative to the population

A small sample size, as it applies to this research, refers to a sample of less than 30 members regardless of the population size (Bock & Sergeant 2002).

Further, Roscoe (1975) suggests that:

- Sample sizes larger than 30 and less than 500 are appropriate for most [quantitative] research
- A minimum sample size of 30 for each category is recommended should the sample be further broken into sub-categories
- For multivariate research, including multiple regression analyses, the sample size should be several times larger than the number of variables in the study
- When undertaking simple experimental research under tight controls, a sample size of 10 to 20 may be successful

(Roscoe 1975)

Within the context of this study, the small sample size impacted upon the types of statistical analysis able to be undertaken by the researcher (as suggested by Roscoe (1975)) and the generalisability of the findings to the entire population.

The large representation of population and small quantity of actual subjects is not suited to all statistical analysis and impacts on the ability to draw conclusions from the data through the use of statistical methods such as;

- Chi squared testing
- T testing
- Multiple regression analysis

However, the data gathered in this research study was provided by 70% of the population. As this provides a large sample it is more likely it is to be representative of the population (Levy & Lameshow 1991). Therefore the data collected in this study will provide benefit as long as care is taken with the analysis and any subsequent recommendations despite its relatively small count.

Results and Analysis

A population of 30 team leaders from 30 organisations that were confirmed as currently undertaking Forensic Computing Investigation was identified. In addition to those organisations outlined above, the researcher further recognises that other organisations may have been participating in Forensic Computing Investigation within Australia. However, in the absence of previous comprehensive research in the area and despite exhaustive enquiries undertaken as a component of this research, no further organisations engaged in Forensic Computing Investigation were identified.

From the 30 surveys distributed, 21 were returned as completed by the respondents.

The overall response rate for this study was 70%, which favourably compares with other questionnaire based Information Systems Research responses reported in the literature that cite around 20% as a valid return rate (Young 2000).

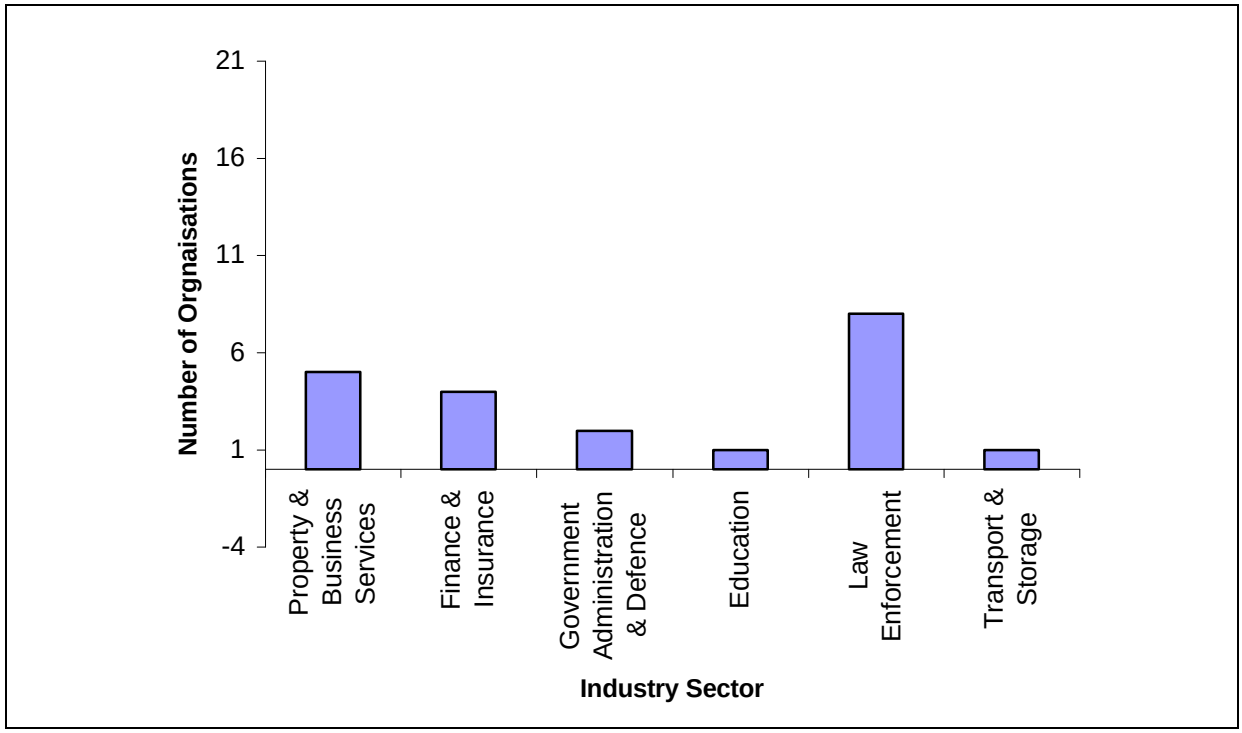
Demographics

Table 2 provides a respondent profile for the study.

Gender					
	N	Frequency	Percent (%)		
Male	21	20	95.2		
Female	21	1	4.8		
Total	**21**	**21**	**100**		
Period Respondent had held current position					
	N	Frequency	Percent (%)		
Less than 1 year	21	5	23.8		
1 year to less than 3 years	21	7	33.3		
3 years to less than 5 years	21	5	23.8		
5 years or more	21	4	19.0		
Total	**21**	**21**	**100.0**		
Years of Experience of Respondent in FCI					
	N	Minimum (yrs)	Maximum (yrs)	Mean (yrs)	Std. Deviation
Years of Experience of Respondent	21	1	15	5.95	4.70

Table 2 Respondent Profile

The sample of Forensic Computing Investigation team leaders in this study provided representation across six industries (see Figure 1). The largest industry involvement came from Law Enforcement agencies (37%) with Education and Transport and Storage having the lowest number of organisations participating in the study with one (5%) organisation each.



(n=21)

(Industry classification source: ABS, 1997)

Figure 1 Industries Represented in Sample

The industry categories were based upon Australian Bureau of Statistics (1997) categories. A majority of 15 (or about 71%) of the Forensic Computing Investigation teams answered that they undertook investigation within the law enforcement industry followed by 10 team leaders (about 48%) nominating the finance industry as being the next common industry their team dealt with. Table 3 provides the frequency for all industries nominated by the team leaders within which the Forensic Computing Investigation teams operate.

Industry	Number of Forensic Computing teams dealing with Industry
Agriculture, Forestry & Fishing	3
Mining	3
Electricity, Gas & Water Supplies	4
Construction	3
Wholesale Trade	4
Retail Trade	6
Accommodation, Cafes & Restaurants	3
Transport & Storage	5
Communications Service	6
Finance	10
Insurance	5
Property & Business Services	5
Government Administration & Defence	7
Education	5
Health & Community Services	5
Culture & Recreation Services	3
Personal & Other Services	4
Ownership of Dwellings	3
Law Enforcement	15

(n=21)

Table 3 The types of industry Forensic Computing Investigation teams deal with in Australia

Team leaders were also asked to quantify the number of full-time equivalent (FTE) employees employed within their Forensic Computing Investigation team. One respondent declined to answer the question citing fear of competitors becoming aware of their organisation's capabilities as the reason for declining to answer. The total number of Forensic Computing Investigators represented in the 20 participating organisations was 95 full-time equivalent employees.

The sample of 20 Forensic Computing Investigation teams had a median of 3.00 FTE employees in each Forensic Computing Investigation Team (Range 0 to 22; Skewness 2.14). One respondent failed to provide an answer to this question reducing the sample to 20 participants.

Competence of Teams

The questionnaire asked the Forensic Computing Investigation team leaders to indicate the types of training or educations that its team had received in relation to each competence and sub-competence area of the expanded taxonomy. They were also asked to provide additional areas of competence not included within the taxonomy and provide the type of training or education for these further competence areas.

Team leaders were also asked to provide an indication of their preference for competence acquisition methods for Forensic Computing Investigation teams. The questionnaire asked the team leaders to rate the competence acquisition methods of Self Education, On the Job Training, Pre-Tertiary Education, Industry Training Course, Internal Training Course, and Tertiary Education

The team leaders preferences were then ranked according to means from most important to least important. Table 4 provides this ranking.

	Mean	Std. Deviation
On The Job Training	5.571	.598
Tertiary Education	4.810	1.167
Industry Training Courses	4.810	1.327
Self Education	4.524	1.289
Internal Training Courses	4.286	1.419
Pre-tertiary Education	2.619	1.161

Scale 1= Least Important – 6 = Most Important (n=21)

Table 4 Respondents rating of competence development methods

Table 5 provides an overall comparison of the importance of competence areas. The column, Current Raw, provides the ranking of the order of importance obtained from the mean of the frequency of competence development methods. This measure provides a raw indication of the importance of the competence areas based upon the quantity of training or education undertaken by Forensic Computing Investigation teams. The Current Weighted column provides the weighted mean of frequencies according to the team leaders ranking of the competence acquisition methods (Table 5). The next column, Current Rank, provides the ranking provided by the respondents for the importance of the current competence areas for Forensic Computing Investigation. The final column gives the ranking from the respondent's rating of the most importance competence areas for Forensic Computing Investigation in the future.

Order of Importance	**Current Raw** *(Based on Frequency)*	**Current Weighted** ***(Weighted Frequency)***	**Current Rank** ***(Mean of Importance)***	**Future Rank** ***(Mean of Importance)***
1	Computer Science	Computer Science	Investigation Skills	Investigation Skills
2	Investigation Skills	Investigation Skills	Computer Science	Computer Science
3	Law	Information Systems	Law	Law
4	Information Systems	Law	Information Systems	Information Systems
5	Social Science	Social Science	Social Science	Social Science

Table 5 Comparison of importance of competence areas

Table 6 provides an overall comparison of Forensic Computing Investigation sub-competence areas. As with Table 5, Table 6 is ordered from highest to lowest according to Current Raw, Current Weighted Mean, Current Rank and Future Rank methods.

Details for additional Forensic Computing Investigation sub-competence areas are provided in the Current Raw and Current Weighted columns.

Order of Importance	***Current Raw (Based on Frequency)***	***Current Weighted (Weighted Frequency)***	***Current Rank (Mean of Importance)***	***Future Rank (Mean of Importance)***
1	Computer Security	Computer Security	Investigation Skills	Operating Systems and Application Software
2	Operating Systems and Application Software	Operating Systems and Application Software	Operating Systems and Application Software	Investigation Skills
3	Investigation Skills	Investigation Skills	Criminal Law	C.C.T. Law
4	Systems Programming and Programming Languages	Systems Programming and Programming Languages	C.C.T. Law	Computer Security
5	Criminal Law	Criminal Law	Computer Security	Criminal Law
6	Systems Management and Polices	Systems Management and Polices	Systems Programming and Programming Languages	Systems Programming and Programming Languages
7	Systems Design and Analysis	Systems Design and Analysis	Civil Law	Civil Law
8	C.C.T Law	C.C.T Law	Systems Management and Policies	Systems Management and Policies
9	Civil Law	Civil Law	User Education	User Education
10	User Education	User Education	Systems Design and Analysis	Systems Design and Analysis
11	Language Skills	Language Skills	Language Skills	Language Skills
12	Psychology	Psychology	Psychology	Psychology
13	Sociology	Accountancy	Sociology	Sociology
14	Politics	Sociology	Psychiatry	Politics
15	Psychiatry	Politics	Politics	Psychiatry
16	Accountancy	Tele-communications		
17	Business	Policing		
18	Computer Forensics	Computer Forensics		
19	Incident Response	Guidance Software		
20	Policing	Psychiatry		
21	Tele-communications	Incident Response		
22	Guidance© Software	Business		
23	Policing	Forensic Science		
24	Electronics	Electronics		

Table 6 Comparison of Forensic Computing Investigation sub-competence importance

Table 6 shows that the Forensic Computing Investigation sub-competence areas of Operating Systems and Application Software are highly rated across all measures of importance. The Forensic Computing Investigation sub-competence areas of Language Skills, Psychology, Sociology, Politics and Psychiatry all rank low on importance among the sub-competence areas from the expanded taxonomy.

Computer, Communications and Technology Law can be seen to increase in importance across the four rankings, with both the Current Raw and Current Weighted rankings substantially lower than the Current Rank rating. Language Skills at ranking 11, is the highest ranked sub-competence area to achieve the same ranking across all ranking methods, however this ranking is quite low.

The weighted mean, as an indication of importance of competence, was calculated for all sub-competence areas and includes the additional competence areas nominated by the respondents as shown in Table 6 and Figure 2. The Figure depicts a high score of importance for the sub-competence areas from Computer Security to User Education. There is a distinct drop in the level of importance between User Education and Language Skills and the remaining sub-competence areas.

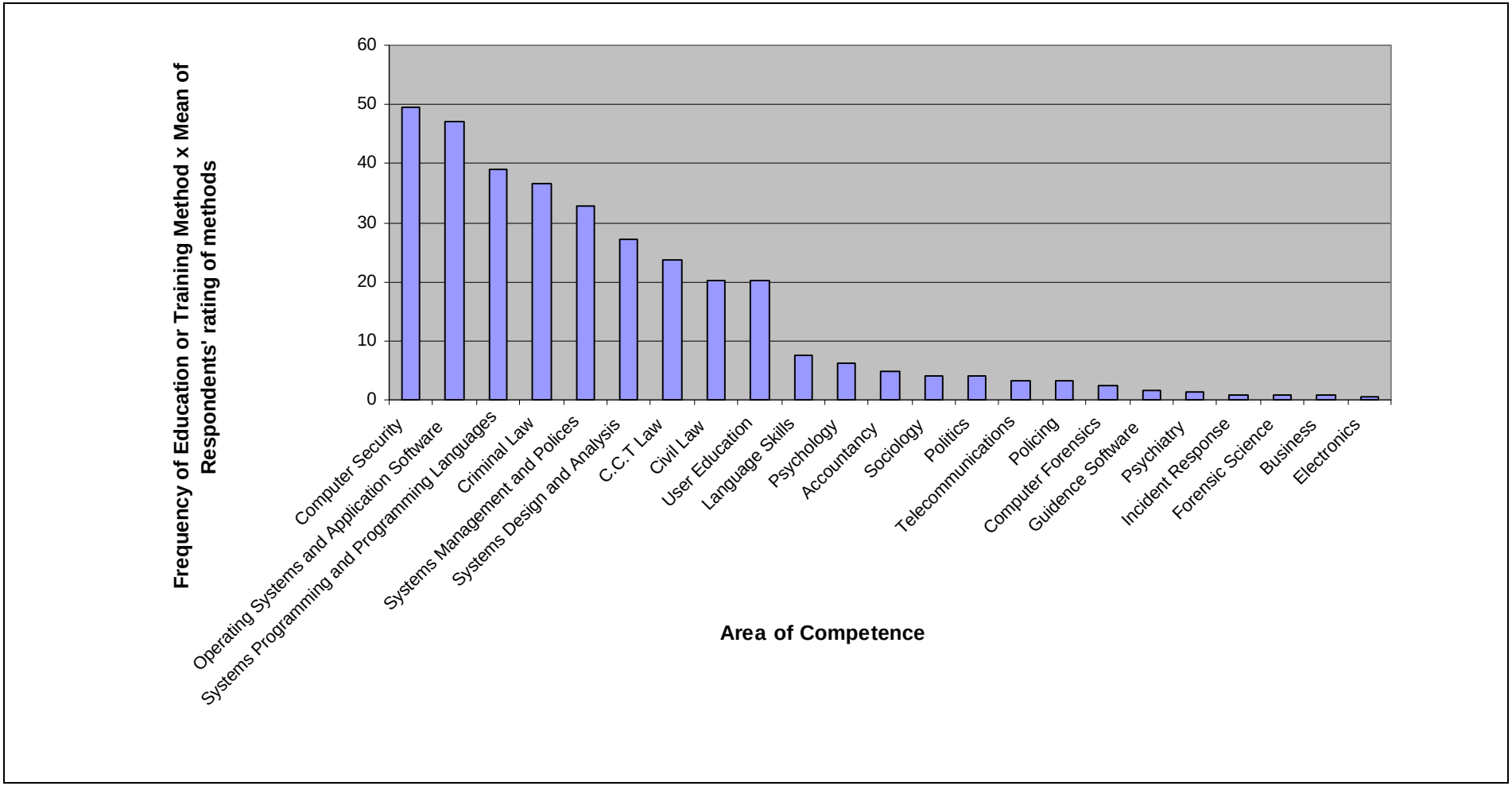


Figure 2 The weighted importance of sub-competence areas (including additional competence areas)

(n=21)

Discussion

The study has shown that a core of competence exists in FCI teams currently conducting Forensic Computing Investigations in Australia. Based on the results for all the respondents, most FCI teams within Australian organisations today possess the competence areas of investigation skills, computer science, information systems, law and social science. However, examination of the weighted frequency of sub-competence areas indicates that the following sub-competence areas form a core among Forensic Computing Investigation teams.

1. Computer Security
2. Operating Systems and Application Software
3. Investigation Skills
4. Systems Programming and Programming Languages
5. Criminal Law
6. Systems Management and Policies
7. Systems Design and Analysis
8. C.C.T Law
9. Civil Law
10. User Education

The competence areas were developed through the expansion of the academic taxonomy developed by Broucek and Turner (2001). Further, the respondents provided the following additional sub-competence areas:

- Accountancy
- Telecommunications
- Policing
- Computer Forensics
- Guidance© Software
- Incident Response
- Business
- Forensic Science
- Electronics

Some of these additional competence areas and sub-competence areas, provided by the respondents, may fall within the competence areas defined within the expanded taxonomy. However, further clarification with the respondents may be required to clarify the exact meaning of the short descriptions provided for these additional competence areas or sub-competence areas.

One respondent provided the competence discipline of Electronics as an additional competence discipline for Forensic Computing Investigation. The respondent indicated that within their Forensic Computing Investigation team, competence had been developed in electronics through pre-tertiary education. Whilst this alone would not add considerable weight to the inclusion of this discipline within an expanded Forensic Computing taxonomy, another respondent indicated that their team outsourced specialist services in the area of specific hardware engineering giving support to its inclusion.

Broucek and Turner (2001) identified that Forensic Computing is not limited to computing and computer technologies but includes digital devices and digital storage mechanisms. The need to construct specific hardware to facilitate the examination of these storage media will also impact upon the role of the Forensic Computing Investigator. The further acceptance of these devices into daily life and law of evidence will require developments of specialist hardware for the purpose of gathering, examining and presenting evidence for Forensic Computing Investigation.

Two respondents specifically listed Guidance© Software as an area of competence additional to the expanded taxonomy. Guidance© Software is the maker of the EnCase© software packages: EnCase© Forensic and EnCase© Enterprise. The software packages provide a range of functions that the manufacturers claim to assist organisations with proactive and reactive Forensic Computing Investigative functions.

The ranking of actual training and education methods for Forensic Computing Investigation competence development differ from the methods most preferred by Forensic Computing Investigation team leaders. However, the preferred and more common method of competence acquisition within Forensic Computing Investigation teams was On the Job Training. The least common or preferred method was pre-tertiary education.

Forensic Computing Investigation teams currently working in Australia developed competence from the following (ranked from most frequent method to least frequent):

1. On The Job Training
2. Self-Education
3. Tertiary Education
4. Industry Training Courses
5. Internal Training Courses
6. Pre-Tertiary Education

The bias towards informal training is likely to be reflective of the juvenile state of Forensic Computing as an academic discipline. This combined with the recent introduction of specialist Forensic Computing teams within organisations has left little time for formal educational institutions to develop and implement structured learning courses to address the requirements of organisations undertaking Forensic Computing investigation.

Conclusions

The rapid uptake of technology within Australia and globally has resulted in the increased opportunity and capacity for individuals and groups to engage in criminal, illegal or inappropriate behaviour using computer related technology. FCI teams have emerged as governments and private organisations rise to the meet the challenges associated with such behaviour.

The report focused on the measurement of competence among Forensic Computing Investigation teams, as they exist within a rapidly changing technological environment. The purpose of these teams is to undertake *post facto* investigation into criminal or other inappropriate conduct committed by the use of, or involving, a computer or electronic device (Broucek & Turner 2001).

In the context of Australia facing the challenge of technology this research provides a body of knowledge relating to Forensic Computing Investigation team competence. Furthermore, future research opportunities exist which build upon the body of knowledge developed in this report.

In addition, this report has identified a generic list of human competence among Forensic Computing Investigation teams. The areas of competence are:

1. Computer Security
2. Operating Systems and Application Software
3. Investigation Skills
4. Systems Programming and Programming Languages
5. Criminal Law
6. Systems Management and Polices
7. Systems Design and Analysis
8. Computer, Communications and Technologies Law
9. Civil Law
10. User Education

This core represents sub-competence areas from the Forensic Computing Investigation competence areas of Computer Science, Investigation Skills, Information Systems and Law. It is envisaged that this list can serve as a source of reference or resource for Australian and international organisations seeking to form or further develop Forensic Computing Investigation teams.

Through the personal contact of the researchers it became evident that many of the people working within Forensic Computing Investigation teams across Australia, regardless of the organisation they currently work for, had developed investigative skills through previous employment with State and Territory Police Services. In addition to this, many team members had worked within Forensic Computing or Fraud Investigation teams within their respective Policing Organisations. This is reflected in the strong bias towards Investigate Skills developed through On the Job Training within current Forensic Computing Investigation teams operating within Australia.

The position of tertiary education as the third most frequent form of competence acquisition is also of interest. The academic discipline of Forensic Computing is still emerging (Broucek & Turner 2001) and no tertiary education institutes within Australia offers specific courses within this field. However, many of the Forensic Computing Investigation team members possess tertiary qualifications within competence areas of Forensic Computing Investigation. This indicates that the teams on a whole comprise team members who possess a high level of formal education.

To fulfil the objectives of this study, it was necessary to develop a competence measurement instrument in order to measure Forensic Computing Investigation team competence within a rapidly changing technological environment. The instrument was based upon traditional competence measurement literature as reviewed in the literature and applied within an environment of rapid technological change. A team leader was used to complete a questionnaire that was developed and administered using the research methodology establishing in Chapter Three of this thesis.

The development of the research instrument and methodology draws on literature from a range of fields including Human Resource Management, Information Systems, Organisational Strategy and Forensic Computing. It is anticipated that the methodological developments undertaken by the researcher can provide guidance for other research that aims to examine team competence within rapidly changing technological environments.

Reference

ABS (1997). Take-up rate for modem and internet use low. Canberra, Australian Bureau of Statistics. 2002.

ACPR (2000). The Virtual Horizon: Meeting the Law Enforcement Challenges - Developing an Australasian law enforcement strategy for dealing with electronic crime. Adelaide, Australasian Centre for Policing Research**:** 1-132.

ACPR (2001). Electronic Crime Strategy of the Police Commissioners' Conference. Adelaide, Australasian Centre for Policing Research.

Babbie, E. (2001). The Practice of Social Research. Belmont, Wadsworth/Thomson Learning.

Barney, J. (1996). Gaining and Sustaining Competitive Advantage. New York, Addison Wesley Publishing Company.

Bassellier, G., Reich, B.H. & Benbasat, I. (2001). "Information technology competence of business managers: A definition and research model." Journal of Management Information Systems 17(4): 159-182.

Bates, J. (1997). "Fundamentals of Computer Forensics." International Journal of Forensic Computing.

Bock, T. & Sergeant, J. (2002). "Small sample market research." International Journal of Market Research 44(2): 235-244.

Boyatzis, R. E. (1982). The Competent Manager: A Model for Effective Performance. New York, John Wiley & Sons.

Broucek, V. & Turner, P. (2001). "Forensic Computing: Developing a Conceptual Approach in the Era of Information Warfare." Journal of Information Warfare 1(2): 95-108.

Dalton, M. (1997). "Are competency models a waste?" Training & Development 51(10): 46-49.

Drucker, S. J. & Gumpert, G. (2000). "CyberCrime and punishment." Critical Studies in Media Communication 17(2): 133-158.

Dubois, D. D. (2000). "The 7 stages on one's career." Training & Development 54(12): 45-40.

Epstein, R. M., & Hundert, E.M. (2002). "Defining and assessing professional competence." The Journal of the American Medical Association 287(2): 226-235.

Etter, B. (2000). Working in Partnership: The Australian Policing Response to Electronic Crime. Cybercrime, Sydney.

Etter, B. (2001a). Computer Crime. AIC 4th National Outlook Symposium on Crime in Australia -

New Crimes or New Responses, Canberra.

Etter, B. (2001b). The forensic challenges of e-crime. Adelaide, Australasian Centre for Policing Research**:** 1-8.

Farmer, D. (2001). "Bring Out Your Dead. The Ins and Outs of Data Recovery." Dr Dobb's Journal 30(1).

Hearn, G., Close, A., Smith, B., & Southey, G. (1996). "Defining Generic Professional Competencies in Australia: Towards a Framework for Professional Development." Asia Pacific Journal of Human Resources 34(1): 44-62.

Henderson, R. M. (1992). Transforming Education. Oxford, Oxford University Press.

Hitt, M. A., Ireland, R.D., & Hoskisson, R.E. (1997). Strategic Management: Competitiveness and Globalization. St. Paul, West Publishing Company.

Levy, P. & Lameshow, S. (1991). Sampling of Populations: Methods and Applications. New York, John Wiley & Sons.

McClelland, D. C. (1973). “Testing for competence rather than for "intelligence."” American Psychologist 28: 1-14.

McKemmish, R. (1999). What is Forensic Computing? Canberra, Australian Institue of Criminology**:** 1-6.

McLagan, P. A. (1997). “Competencies: The next generation.” Training & Development 51(5): 40-47.

Murlis, H. F & Fitt, D. (1991). “Job Evaluation in a Changing World.” Personnel Management 23(5): 39.

Neuman, W. L. (2000). Social Research Methods. Boston, Allyn and Bacon.

NOIE (2000). E-commerce beyond 2000, National Office for the Information Economy. 2002.

O'Rourke, T. (2000). “Practical sampling for health professionals.” American Journal of Health Studies 16(2): 107-109.

Prahalad, C. & Hamel, G. (1990). “The core competence of the corporation.” Harvard Business Review: 79-91.

Probst, G., Raub, S. & Romhardt, K. (2000). Managing Knowledge. West Sussex, John Wiley and Sons.

Reno, J. (1996). Law Enforcement in Cyberspace Address. Internet Besieged: Countering Cyberspace Scofflaws. D. E. D. P.J.Denning, ACM Press**:** 439-447.

Robson, W. (1997). Strategic Management & Information Systems. Harlow, Prentice Hall.

Roscoe, J. T. (1975). Fundamental research statistics for the behavioral sciences. New York, Holt, Rinehart and Winston.

Schippmann, J. S., Ash, R.A., Carr, L., Hesketh, B., Pearlman, K., Battista, M., Eyde, L.D. Prien, E.P., & Sanhez, J.I. (2000). “The practice of competency modeling.” Personnel Psycology 53: 703-740.

Venema, W. (2000). “File Recovery Techniques. Files Wanted, Dead or Alive.” Dr Dobb's Journal 29(12).

Ward, J. & Griffiths, P. (1996). Strategic Planning for Information Systems. West Sussex, John Wiley & Sons.

Woodruffe, C. (1991). “Competent by Any Other Name.” Personnel Management 23(9): 30.

Young, J. (2000). The career paths of C.S. and I.S. Major Graduates. School of Information Systems. Hobart, University of Tasmania**:** 355.