Proceedings of the 8th Colloquium for
Information Systems Security Education
West Point, NY June 2004

Infosec Education and Expert Witnessing

William J Caelli, Sen MIEEE and Caroline L Allinson

Education and training in the discipline of information assurance must allow for a dual approach to this activity. This dual approach becomes clear when the problem of "expert witnessing" in the information technology area during legal proceedings is considered. The basic concern lies in the need to clarify educational objectives against a background of two different and often opposing "market" demands on the education and training process as well as on the underlying discipline content. The two opposing "forces" may be categorised as firstly the "computer science and engineering (CSE)" or "base technology" approach while the second may be identified as the "information systems (IS)" or "business requirements" approach, mirroring the debate in the general IT education arena. These differing approaches may also serve differing enterprise needs. One approach, the CSE approach, may be seen as addressing the needs of the information and communications technology (ICT) industry itself as well as broad governmental and defence requirements for educated investigators in this field. The second approach, the IS approach, may be seen as handling the needs of users of the products, systems and services of the ICT industry in an extremely broad variety of other enterprises, both public and private. This paper argues that these separate approaches to information technology education may not individually serve the information security profession well as aspects of both are seen as being critical to a professional assessment of the state of the information assurance and security position of any enterprise. In particular, such a integration of approaches must be achieved, in base education in the ICT area, in order for the information security professional to be considered an essential part of any enterprise and, indeed, to be recognised as an "expert" in legal and like proceedings. Specialist areas then need to be catered for by associated specialist courses mirroring current practice in other areas such as medicine, etc.

Index Terms—Expert Witness, Information Assurance

I. Introduction.

Education and training in the information technology area and the expanding discipline of information assurance/security studies are exhibiting a "*split personality*". This problem comes into clear focus when the requirements for "*expert witnessing*" in legal proceedings with relevance to the information technology area are considered. The basic problem lies in the need to clarify and cater for dual educational objectives against a background of two different and often opposing "*market*" demands on the education and training process as well as on the underlying discipline content. The two opposing "*forces*" may be categorised as firstly the "*computer science and engineering (CSE)*" or "*base technology*" approach while the second may be identified as the "*information systems (IS)*" or "*business requirements*" approach. These dual characteristics mirror the debate in the general information technology (IT) education arena but become of particular significance in relation to education and training in the information assurance speciality. This paper proposes that both approaches are necessary. However, as in other professions, particular emphasis and choice must exist to allow for students to be able to specialise. In this way the perceived needs, for example, of expert witnessing in courts of law may be more readily met with recognition of specialist areas becoming easier, as is the case in other disciplines such as medicine, pathology, etc. The separate approaches are considered in more detail below in relation to the case of more general education in the IT discipline.

II. Information Systems Approaches to Information Assurance.

It is instructional to look at a typical introductory text book from the end of the 1990s to check just what approach is taken to the topic of information systems security and related governance matters in a teaching text of the period. The Fourth Edition of the "*Principles of Information Systems*" by Stair and Reynolds [1] is a case in point. The area of information security is only partially covered and then in the last chapter of the book, Chapter 14, Pages 627 to 659 in a book of over 700 pages. That chapter, giving the impression of "*the last thing to be considered*" by its location just before a thesaurus, also covers diverse topics including furniture ergonomics in the same chapter. Obvious and appropriate information systems topics such as risk assessment and management, corporate and IT governance, legal requirements and the like get little to no coverage and the whole concept of system security evaluation gets no mention at all. This last situation indicates that the authors had no interest in or knowledge of such topics as the "*Common Criteria*" standard for system

Professor William J Caelli, AO, BSc(Hons), PhD, FACS, FTICA, Sen MIEEE, CISM is the Head of the School of Software Engineering and Data Communications at the Queensland University of Technology, Brisbane, Queensland, Australia. Ms Caroline Allinson, M Inf Tech, B Bus, CISSP, CISM, CISA is a Doctoral student in the Information security Research Centre at the Queensland University of Technology, Brisbane, Queensland, Australia.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

evaluation as a metric. Meanwhile, protection of networked computer systems is seen as an "*Internet*" or network problem and the text advises that information systems professionals should advise that external Internet security specialists be brought in as required by any enterprise. Indeed, overall system security in this networked environment is seen as a "*network*" problem, not a computer system or node problem. Again, topics like governance, risk assessment, etc. are not even indexed.

This, then, sets the "*scene*" in relation to introductory information system oriented text books and possible related education classes at the end of the 20th century. Since then, with the passing of the "*Sarbanes-Oxley Act*" in the USA, etc., the topic of responsibility for corporate, and thus IT, governance has entered the legal arena. In this regard, an emphasis is rightly placed on an understanding of the basic information needs of the enterprise through a thorough assessment of its business activity coupled with an assessment of the underlying security regimes that must exist to protect such information assets. The primary interest in this case is the use of IT system to meet fundamental enterprise information service needs, internally within as well as externally to the organisation. Thus pressures are placed on academics to align education programs in the information systems discipline to meet perceived industry needs including organisational considerations, team work, market orientation, speed of implementation and cost containment for new systems development and deployment, etc. At the same time, students may be encouraged to undertake cross-discipline courses in such topics as accountancy, marketing, human resource management, and the like. Thus an educated information systems professional should be seen as being capable and competent in all aspects of an enterprise's information systems needs and thus able to represent that enterprise in any legal proceedings that may arise in this area.

III. Computer Science and Engineering Approaches to Information Assurance.

In contrast, the traditional scientific, technological and engineering approaches to information assurance and security have classically emphasized areas such as computer and data network architectures, cryptology and cryptographic protocols, network security and management, access control schemes and the design of operating systems, and the like. These approaches, while essential in most ways, had to de-emphasize such topics as enterprise information systems development, relevant law and regulations, human behaviour in a corporate environment, sociology of medium to large organisations, and the like. Text books in this sector were notable in the mid-to-late 1990s and on. These include:

- *"Security Engineering: A Guide to Building Dependable Distributed Systems"* by Ross J. Anderson, 2001 [2], and
- *"Practical UNIX Security"* by Simson L. Garfinkel and Gene Spafford, 1991, with its 2nd edition, renamed *"Practical UNIX and Internet Security"* in 1996, with a 3rd edition, with S. Garfinkel and A. Schwartz in February 2003 [3].

This technological approach to information assurance education may be considered, for example, as being essential from national security and crime prevention viewpoints. The reason for this is the fact that such education is essential, for example, in enabling professional analysis of underlying limitations and vulnerabilities inherent in commercial-off-the-shelf (COTS) products and services. At the same time, the assessment of the level of the risk that such vulnerabilities may be exploited to compromise vital, national information systems in which such products are used can also only really be done following education at this basic technological level. In simple terms, basic ICT education must form the ability of the relevant ICT professional to assess the level of technological skills needed by an adversary to perpetrate an attack. Of course, such topics as development of an understanding of the likely motivation for the mounting of attacks on national information infrastructures, etc. must come into education in relation to the overall risk "*equation*". This, in turn, involves a study of topics in basic sociology, psychology, political science and like disciplines and illustrates the point that the two approaches considered in this paper do, at times, complement each other.

IV. The Requirements for Expert Witnessing in Court and Allied Legal Proceedings.

While the above has considered the separate aspects of CSE and IS approaches to information assurance education with an emphasis on business and national security needs, these two become important when consideration is given to the likelihood of an IT professional being called to act in a court of law as an *"expert witness"*. In clarifying the needs of information assurance education in the early 21st century it is useful to consider such a legal situation. In this regard, however, there are problems concerning the matter of expert witnessing in relation to the discipline of Information Technology (IT). For example, from a legal viewpoint and unlike the cases of traditional Forensic Science and Medicine, there are very few formally defined, accepted and relevant specialities within the overall IT discipline itself. In relation to the law and relevant legal proceedings, IT is separately identified and categorized but to date nothing appears to have been established in any national or international forum in the form of professional recognition and accreditation for expert witnesses within this discipline. It may be argued that, given the ubiquity of IT in all aspects of public, enterprise and personal affairs, clear

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

identification and codification of matters relating to the provision of "*expert witness*" services in IT to legal proceedings is now an urgent requirement.

The World Book Dictionary defines the word *"expert"* as *"a very skilful person who knows a great deal about some special thing"*. When used as an adjective *"expert implies having mastery or unusual ability as the result of experience in addition to training and practice"* (1974). In defining an expert in legislative terms, most Evidence Acts require that a witness, qualified as an expert, must be so in knowledge, skill, experience, training, or education, as stated by Wagner and Weil [4].

In the court system, experts have a privileged position. As the above definition implies they must be reputable people with ability, training and experience which together form part of a *"body of knowledge"* which is recognized in society as belonging to an identified and reliable discipline. Within this, and some other set rules, they are allowed to give evidence to a court in the form of *"opinion"*. This latter factor is a vital part of the definition of an expert.

History shows that the concept of expert evidence has been around for hundreds of years. However, within the legal fraternity there is much discussion, argument and challenge as well as calls for reform in relation to the acceptance of designated experts and related expert evidence in the IT area. There appears to be a general perception that all persons involved in IT may be regarded as "*experts*" in this discipline in all its aspects and variety. This is not only untrue but it is a dangerous and potentially damaging misconception. Generally understanding all instances of "*IT*" to be a "*profession*", and one considered to be less than 50 years old, has a number of relevant and serious flaws.

The discipline or practice of IT must be considered as being extremely diverse in nature. At the very simplest level, anyone in the global community can set themselves up in the IT business and offer IT products and services apparently without any training, education, qualifications or experience. In this regard general practice in the IT profession must be considered to be mainly unregulated by any governmental or equivalent authority on a global scale. This is totally at difference to other recognised professions such as medicine, veterinary services, legal practice, accountancy, and so on. With the movement of IT products, both hardware and software, to "*commodity status*" over the last 20 years or so this essentially "*laissez-faire*" attitude and trend by government has accelerated. At the same time this fact appears to be acceptable in today's society and to today's governmental and regulatory authorities. Given this situation, the ability for courts to determine just who is a legitimate IT "*expert*" within the rules of expert evidence is limited and of concern. The lines are blurred and even the IT industry and profession appear to be confused in this regard. It must be emphasized that the appearance of an "*IT expert*" in legal proceedings would normally only occur in the case of commission of crime, major commercial dispute, or the like. This means that essentially such an IT expert will most likely be involved in offering "*opinion*" related to the assurance and security of information technology products, systems and services in some form.

IT has now been recognised for several decades as a profession and can definitely be defined as a reliable discipline with a recognized body of knowledge. Professional societies have been established worldwide, introducing professional accreditation, an ethical stance and sets of codes of conduct for recognised IT professionals. For at least the past three to four decades academic institutions at tertiary education level have established schools or departments specifically related to information technology, offering both under-graduate and post-graduate qualifications in the area. However, titles for these educational activities have varied from "*computer science*" to "*information systems*" to "*data communications*" to "*computer engineering*" and so on.

At the same time, the last decade has seen a massive development in *"industry certification"* programs with associated industry defined bodies of knowledge and assessment processes, particularly in the information security area. These programs are offered not only by individual IT companies, in conjunction with their more normal product and service supply activities, but also by a number of "*not for profit*" and allied enterprises aiming at broader industry acceptance of their qualifications.

In summary, education and training activities in the IT area today fall into the three broad categories of:

- Offerings by traditional tertiary educational institutions, such as universities, colleges and the like,
- Courses offered by a number of corporate entities that are not tied to a particular IT product or services vendor, and
- Training, and even more advanced and more general IT education, provided by IT product and service manufacturers and vendors.

Unfortunately, in relation to the problems facing the clarification of expert witnessing in the IT area, there exists a fringe element of individuals who claim to be, or genuinely are, self taught. However, with very little to no demonstrated or tested expertise in the more specific and relevant areas of IT required in legal proceedings, they may still set themselves up and claim to be IT professionals. In such cases, true professional ability may be indeed questionable and even totally lacking. To date, enterprises, both public and private, as well as governments and society in general, have allowed this to occur. These matters set a background for the dual nature of IT education mentioned

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

above and provide a focus for discussion on relevant syllabi needed for education in the information assurance area.

The IT industry does not have the tradition or impetus as yet that the medical, legal and accountancy professions, for example, have in relation to this ability to practice. For example, a medical professional must achieve certain qualifications and have designated, supervised work related experience before entering into the profession on a "*solo*" or like basis. Membership of an appropriate medical "*college*" may also be required. Moreover, governmentally imposed "*registration*" requirements covering such professions may exist at local, regional or national levels. If such a registered person breaches a relevant code of conduct, or is guilty of proscribed misconduct or the like, he/she can be struck off a "*register*" and banned from practicing medicine, for example. Similar requirements apply in the legal profession.

This is not the case in IT. Persons can establish themselves in the industry and claim to be a "*professional*" at any level chosen. For example, IT employees and/or students have committed computer related crimes and in some instances have then been hailed as "*heroes*", becoming infamous for their activities. These same people have later even been employed by governments to advise on information security matters (See: URL http://www.kevinmetnick.com). This matter has particular bearing in relation to the acceptance of an individual as an "*expert*" in a court of law.

V. Dual Aspects of the IT profession.

There are a number of peculiarities in the Information Technology area. Information technology is an extremely diverse area of expertise and one which is not very well controlled from social or legislative points of view. Therefore, it is worth considering several aspects of the overall societal functions of IT professionals in relation to peculiarities within this discipline when discussing the problem of expert witnessing at court and education requirements that arise from that consideration.

The relevance of an IT expert in relation to witnessing in specific legal proceedings may be more related to their role and function in an organisation making specific use of the products and services of the technology. Specific training and expertise in the underlying or fundamental principles as well as the details of a given technology and its artifacts may be less important in this case. This occurs because a relevant matter before a court, as seen so far, is most likely to be related more to an occurrence affecting a business activity or the implementation and control of IT in the organisation in question. In certain circumstances, such as product liability cases, disputes involving patent, copyright or intellectual property rights, packaged software quality and performance, external penetration of systems, etc. the situation may be one where specific technical and even scientific knowledge and experience may be required. However, in normal business practice such situations would normally be seen as related to the IT products and services industry itself rather than to the enterprises making use of IT for its normal activities. The instantiation is the event and matter at hand before the court. It would be unusual for a court to delve deeply into the background and expertise of an expert witness in specific technologies unless this has specific bearing on the case. It must be noted in this regard that the amount of variability and complexity in IT could easily outweigh the circumstances that prevail in the case of the use of more traditional expert witnesses. For example, a firearms/ballistics expert has a defined set of limited variables with which to work.

Thus, the legal imperatives of expert witnessing in the IT arena highlight the dual nature of IT assurance education mentioned above. In information assurance education, it appears essential now that both approaches need to exist with options for students to specialise as required. However, the CSE approach detailed above would appear to be necessary when consideration is given to external attack on national information infrastructures since, in this case, such attacks may be clearly based upon exploitation of fundamental vulnerabilities in specific products and systems. The IS case, involving understanding of the information environment of an enterprise, could be seen as less relevant.

VI. Adjusting Training and Education for Emerging Needs.

Given the above, the Queensland University of Technology's School of Software Engineering and Data Communications (SEDC) has commenced a preliminary evaluation of relevant education programs offered in the light of potential expert witnessing imperatives that could fall on its graduates as well as needs for information assurance education in a national information infrastructure protection (NIIP) environment. As explained in the introduction to this paper, clearer separation of the needs of information systems and business analysts are being considered against the technology orientation of other students. In the 2004 to 2005 period new introductory courses are being introduced that address the expert witness problems mentioned above. In addition, new emphases, where relevant, are being made in existing courses. It is simply recognised that graduates in information security, in particular, may have a high probability of being called to court at some point in their careers to either act as expert witnesses or to become general witnesses in legal proceedings. In this latter case, different rules apply as to the type of evidence that may be given by the IT professional in that, if not presented as an "*expert*", evidence given must be limited to "*facts*".

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

The courses offered may be categorised into the two main areas mentioned above, i.e. "*information systems (IS)*" orientation versus a "*computer science and engineering (CSE)*"orientation, as shown in Table 1 below.

Table 1: Categorisation of Courses Offered at the Queensland University of Technology (2004)

Course ("*Unit*") Code & Status (Under-graduate or Post-graduate) – U/P	Name	Category
ITB646 (U)	Cryptographic Fundamentals	CSE
ITN682 (P)	Advanced Cryptology	CSE
ITB623 (U)	Information Security	CSE & IS (?)
ITN663 (P)	Information Security Management	CSE & IS (?)
ITB645	Network Security	CSE
ITN670	Security Technologies	CSE
ITN681	Trusted Systems and Networks	CSE
ITN673 (P)	Computer Forensics	CSE & IS

The (?) note in the above table against the category indicates that certain pre-requisites for the course may be required and that these pre-requisites may not have been successfully completed by information systems and business oriented undergraduates. It is emphasized that this is a preliminary paper discussing the needs for such an evaluation of programs offered where an emphasis is made on information assurance and security. Some of the courses indicated in the table above have been offered for 15 years or more. This full assessment will be undertaken over the next twelve months, from mid-2004, against the demands outlined in this paper.

A preliminary analysis has indicated that new courses, known as *"units"* at the Queensland University of technology will be needed in the near future. Each of these units involves class contact hours of around 40 hours per week during a 13 week semester. In particular, new units in information assurance oriented more towards business and information system students are essential. In particular, these new units will need to address the concerns related to "*expert witnessing*" addressed in this paper.

VII. Conclusions.

This paper has identified two separate requirements in relation to information assurance and security education and training as a result of analysis of requirements for "*expert witnessing*" in legal proceedings. These may be classified as *"computer science and engineering (CSE)"* and *"information systems (IS)"* approaches. When analysed against the emerging requirements for IT professionals to appear in relevant court or allied legal proceedings, IT professionals may again be divided into two similar categories, i.e. those with "*in-depth*" knowledge of the information resources and processes within a specific IT user enterprise and those with detailed knowledge of the IT products and services in use. This dual approach would also seem to apply in relation to education programs required for those professionals to be involved in national information infrastructure protection (NIIP). These trends indicate a need for a review of both undergraduate and postgraduate education programs in the information assurance/security area.

Sections of this paper have been presented in a thesis by one of the authors, C. Allinson, for the degree of Doctor of Philosophy at the Queensland University of Technology, Brisbane, Australia.

VIII. References

[1] Stair, R. M and Reynolds, G. W. *"Principles of Information Systems"*, Fourth Edition, Course Technology / ITP, 1999, ISBN 0-7600-1079-X

[2] Anderson, R J, *"Security Engineering: A Guide to Building Dependable Distributed Systems"* , John Wiley & Sons, 2001, ISBN 0-471-38922-6

[3] Spafford, G., Garfinkel, S. and Schwartz, A. *"Practical Unix & Internet Security"*, 3rd Edition, 2003, O'Reilly & Associates; ISBN: 0-596-003234

[4] Frank. P. B., Wagner M.J. and Weil, R. L., *"The Role of Accountant as Expert"*, 2nd Edition, 1992, John Wiley and Sons.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE