The Role of Information Security Industry Training and Accreditation in Tertiary Education

Helen Armstrong[1], Colin Armstrong[2]

[1] Curtin University, Hayman Road, Bentley, Western Australia
[2]Gailaad Pty Limited, Perth, Western Australia
[1]H.Armstrong@cbs.curtin.edu.au
[2]ColinArmstrong@gailaad.net.au

Abstract. This paper presents a proposal for a working group session on the role of industry training and professional certification in information security education at the tertiary level. The main question posed is *Does industry training and professional certification have a place in university information security courses?* If so, *What industry training and professional accreditation courses are appropriate?* and *What is the place of these in academic courses and why?* The discussion will centre on three areas: first, the nature of the linkage between industry requirements and academic offerings at university, and secondly the relevance of industry training and professional certification, and thirdly, the role industry training and certification should play in information security university courses.

Keywords: Information security education, information security industry training, information systems professional certification.

1 Introduction

The relevance of industry training and certification materials in tertiary level information security courses has been a matter of regular discussion over the recent past, with most of the written debate published in conference proceedings. Fueled by diminishing government funding for tertiary education institutions and a desire by computing and professional organizations to increase adoption of their products, the character of information systems and information security education is changing.

Alan Stanley in his invited talk at the SEC 97 conference discussed the changing nature of information security and its increasing challenges in meeting the needs of business in a rapidly changing technological environment. Stanley states the complexity and depth of coverage of the information security area as applied in business “is one of the most intellectually challenging topics”[1].

The NSA in the USA has recently published their desire to recognize US institutions that have plotted their information assurance curriculum to US standards

[2]. This is certainly an incentive for US tertiary institutions to align their educational content with national standards. There is evidence of an increased level of alignment of information assurance curricula with industry training, standards and professional bodies (both national and international). Specific examples can be found in the discussions of Rasmussen & Irvine [3], Armstrong & Murray [4], Klevenger & Alexander [5], Taylor, Alves-Foss & Freeman [6], Schembari [7], and Slay [8].

The lack of security in computerized systems and processes that surround those systems has been the focus of extensive discussion for several decades. In the quest to achieve more secure information systems Conti and others [9] state we must provide the appropriate information security education to the people who have to build these systems.

In the experience of Rasmussen and Irvine [3] the education and experience of the personnel involved in product certification and accreditation is critical. They state that qualified personnel are in short supply and in response have established an educational program for certifiers in their DoD environment which includes qualifying for numerous professional body certifications.

The lack of industry-standard skills in network security together with the shortage of expertise in information security has been highlighted at an international level [4] and education and training has been proposed as a means of addressing the shortages of qualified personnel in industry [10].

Incorporation of industry-based training into academic courses is becoming more prevalent. There are many advantages supporting this adoption - for example, provision of skills which are immediately applicable in industry, attraction of more students to educational programs which provide marketable skills, and recognition of educational institutions as ‘relevant’ by organizations in industry.

The question arises – Is there extensive and justifiable support for the alignment of academic courses with professional accreditation and industry-based skills in information security or are we blindly embarking on this activity with little consideration of the consequences?

There is an ongoing debate of Universities claiming that they are providing education while industry courses only provide training. The students desire a University qualification but also want to have actual, practical and applicable skills that they can deploy immediately. They can thereby impress their employer with both education and training qualities. How best academia can accommodate vendor specific and professional accreditation training with academic learning outcomes and broader educational requirements, whilst still satisfying student desired outcomes and meeting international accreditation standards? This venue offers an opportunity to further discussion on these areas.

Some concerns and warnings (for a range of reasons) have also been presented on the topic. Academic institutions need to be aware of the risks associated with such

moves and ensure they continue to offer information security education characterized by a balance of theory, knowledge and skills as part of the life-long learning process [4].

The lack of academic rigor and sound theoretical foundations are the concerns of numerous authors. Rannenberg [11] presents two main disadvantages of IT security product certification – the weaknesses of the underlying security models and the high cost of certification, and both these factors are also relevant to the discussion regarding professional certification of information security professionals. Valli [12] highlights the risks and warns against the consequences of the emphasis on accreditations and focus on industry certifications and encourages educational institutions to consider the consequences seriously - in particular the failing to provide sound foundations and become savants to vendors and industry bodies.

2. Proposed Workgroup Discussion

The first stage in the discussion will be to identify those industry certification, industry training, professional accreditation, and international standards, that have a direct relationship with information security education.

The second stage will be a discussion of the relevance of these in the meeting of academic objectives of tertiary education courses of information security. This will involve identifying the advantages and disadvantages, and weighing up the results.

The role of these professional accreditations and certifications in tertiary level academic qualifications will then be discussed, debating the extent to which these certifications should drive the design of academic programs.

The final stage will be developing guidelines and an action plan.

In order to encourage further discussion of the topic, it is intended that the results of the workshop will be written up into a paper for publication in the information security field.

References

1. Stanley, A.K., Information Security – challenges for the next millennium, in Yngstrom, L. & Carlsen, J., (Eds), *Information Security in Research and Business*, Chapman and Hall, London, (1997), pages 3-8
2. NSA, IACE Courseware Evaluation Programs, http://www.nsa.gov/ia/academia/iace.cfm
3. Rasmussen, C., Irvine, C., Dinolt, G., A Program for Education in Certification and Accreditation, in Irvine, C. & Armstrong, H. (Eds), *Security Education and Critical Infrastructures*, Kluwer Academic Publishers, (2003), pp 243
4. Armstrong, H. & Murray, I., Incorporating Vendor-based Training into Security Courses, *Proceedings of IEEE Systems, Man and Cybernetics Information Assurance Workshop*, June 2005
5. Clevenger, G. & Alexander, T., Practical Curriculum for the Future ISSO, *Proceedings of the 10th CISSE*, 2006, pages 8-13

6. Taylor, C., Alves-Foss, J. & Freeman, V., An Academic Perspective on the CNSS Standards: A Survey, *Proceedings of the 10th CISSE*, 2006, pages 39-46
7. Schembari, N.P., A University Course in Information Systems Risk Analysis/ Security Certification and Accreditation, *Proceedings of the 10th CISSE*, 2006, pages 22-30
8. Slay, J., Embedding Industry Standards within the Undergraduate IT Security Curriculum: An Australian Implementation, *Proceedings of the 8th CISSE*, 2004, pages 71-76
9. Conti, G., Hill, J., Lathrop, S., Alford, K. & Ragsdale, D., A Comprehensive Undergraduate Information Assurance Program, in C. Irvine and H. Armstrong (Eds), *Security Education and Critical Infrastructures*, Kluwer Academic Publishers, (2003), pp 243-260
10. Spalding, E., 2002, European ICT skills shortage still significant, despite economic woes, Comptia, available http://www.trainingpressreleases.com
11. Rannenberg, K., IT Security Certification and Criteria, in Qing, S. & Eloff, J., (Eds) *Information Security for Global Information Infrastructures*, Kluwer Academic Publishers (2000), pages 1-10
12. Valli, C., Industry Certifications, Challenges for the Conduct of University Security Based Courses, *Proceedings of the 4th Australian Information Warfare and Security Conference*, Adelaide, 2003