Toward User Evaluation of IT Security Certification Schemes: A Preliminary Framework

Nicholas Tate[1], Sharman Lichtenstein[2],and Matthew J. Warren[2]
1 Faculty of Science and Technology, Deakin University
221 Burwood Highway, Burwood, 3125 Australia
n.tate@its.uq.edu.au
2 School of Information Systems, Deakin University
221 Burwood Highway, Burwood, 3125 Australia
{sharman.lichtenstein,matthew.warren}@deakin.edu.au

Abstract. This paper reports a preliminary framework that supports stakeholder evaluation, comparison and selection of IT Security Certification schemes. The framework may assist users in the selection of the most appropriate scheme to meet their particular needs.

1 Introduction

Information technology (IT) security certification is of increasing importance to organisations seeking a professional approach to information security management [1]. In the Western world, employers are increasingly relying on IT security certifications - and higher education (HE) qualifications based on such certifications - as key selection criteria in the recruitment of IT security professionals. However, by September 2006 there were around 100 vendor-neutral certifications and around 40 vendor-specific certifications [2]. While these numbers include a broad range of certifications and are, therefore, not always equivalent - they present a bewildering array of schemes from which key stakeholders (such as IT security practitioners and their employers) must select the most appropriate scheme to meet their individual needs.

Currently, such selection must rely only on information available from expert accounts such as [2] or on classifications and approaches such as [3, 4, 5, 6, 7]. Such approaches are not systematic, however. This paper develops a preliminary framework of categories and characteristics to support an evaluation and comparison of IT security certification schemes. The framework is intended for use by the four

Please use the following format when citing this chapter:

Tate, N., Lichtenstein, S., and Warren, M., 2007, in IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer), pp. 473–478.

key constituent audiences – IT security practitioners, employers, HE institutes and government agencies (hereafter termed "users"). It aims to assist users in understanding the relative merits and positioning of each scheme, and assist in the selection of the most appropriate scheme for individual needs. The framework was developed from a literature review and focus group of industry, academic and government stakeholders, held at the AusCERT2006 conference in Australia in May 2006. Next, we review a set of categories and characteristics that underpin the framework.

2 Categories and Characteristics

2.1 Credibility

For a scheme to be accepted by a user, it must be perceived as credible [12]. Three characteristics for credibility are: *governance*, *assessment* and *curriculum definition*. First, if the *governance* of an organisation that offers a particular certification scheme is not open and transparent - with few, if any, conflicts of interest - the scheme is unlikely to gain sufficient user credibility. In addition, if governance of the scheme is not seen to guarantee its independence from any particular commercial, government or national interests, the scheme is likely to suffer diminished credibility. The importance of scheme governance is illustrated by the proportion of the ISO/IEC 17024 standard - ISO/IEC 17024 [16] - devoted to the rules for governing bodies of certification schemes. This standard also states: "The certification body shall be structured so as to give confidence to interested parties in its competence, impartiality and integrity."

Second, the credibility of a certification scheme is linked to its *assessment*. Schultz [15] suggests that many schemes are too simplistic in their assessment requirements. Third, the IT security *curriculum definition* underpins the Body of Knowledge for an IT security professional and is therefore an important credibility characteristic [1, 15]. In particular, the body of knowledge should include discussion and assessment of technological, legal and ethical aspects of IT security [11]. It must also be current and based on relevant international standards.

2.2 Accessibility

It is important that an IT security certification scheme is accessible to potential users. The accessibility of the scheme and the extent to which there are financial or other constraints may be a differentiating factor between schemes when an inclusive approach to evaluation of educational programs is adopted [9] and, for some users, will form an important aspect of evaluation. Three characteristics of accessibility are: *access restrictions*, *cost* and *national restrictions*.

First, in respect of *access restrictions*, an open certification scheme enables individuals to demonstrate their IT security capabilities, irrespective of training. Access restrictions are in place when it is mandatory that a candidate for certification examination first undertake a particular training course, thereby increasing costs and imposing further constraints. Second, user selection of a certification scheme is likely to be linked to the financial *cost* of access. In the case of international schemes, the notion of affordability varies by economy. It is suggested that a scheme which does not account for such variability is likely to limit user access to the scheme. The increasing importance of all the elements comprising the cost is, as reported in [14], amply illustrated by the practice of determining a Return on Investment (ROI) for the certification.

Third, as cybersecurity becomes increasingly important and linked, in the perception of many, to national security, there has been some debate as to whether *national restrictions* should be applied to the selection of candidates for IT security courses. Frincke [13] poses the question, "Who should be allowed to listen?" and observes that "Many security programs already segregate their audiences to a certain extent, for certain material. There are many examples. Some US agencies limit participation to those with US citizenship". In other words, only US citizens may be taught in some IT security courses. An interesting and important question can therefore be posed: is it possible to have a global IT Security certification scheme if certain aspects of it are limited to citizens of a particular country?

2.3 Relevance

For a scheme to be accepted it must be perceived as relevant by (a) IT security professionals who will seek to be certified under it, (b) the employers who may wish to rely on it for selecting staff, and (c) the national jurisdiction in which it operates. Five key relevance-oriented characteristics are: *vendor neutrality, academic credentials and experience, ethical code, market acceptance* and *localisation.*

First, regarding *vendor neutrality*, certification schemes may be differentiated by the providing organisations. There are schemes provided by vendors, which concentrate on certifying that the certification holder has knowledge relating to a particular product from a vendor. There are also schemes which certify broad knowledge of a particular domain, that are generally run by an industry or "not-for-profit" group. Second, regarding *academic credentials and experience*, a key question for a certification scheme is "What are its objectives?" and how does the scheme relate to an academic degree in IT security? Experts suggest that vendor-neutral certification is both complementary to, and an extension of, a degree in IT security by generally requiring a degree, a level of experience and some specific knowledge of professional practise in IT security, which would not normally be included in a degree. Vendor-specific certification is generally regarded as not directly linked to either, but rather, skills training for particular equipment.

Third, most established professions have adopted an *ethical code*. With IT security, a code of ethics can assume particular importance since the knowledge that is needed to defend systems and networks against attack is the same knowledge that could be used to attack them [14]. The need for a code of ethics appears to be met by vendor-neutral certification schemes that mandate agreement to their code. Fourth, if a scheme does not gain *market acceptance* from employers and governments, the scheme will lose relevance and use [10]. Fifth, *localisation* is important as if a scheme does not account for local variations in law, culture, regulation and market development, it is unlikely to be relevant to the jurisdiction in which it operates. The APEC IT skill Report [3] identifies local requirements as key to the relevance of a scheme. It is noted that a number of certifications originate in the USA and, in some cases, their curriculum is based on US legal practice rather than international needs.

3 Toward an Evaluation Framework

A preliminary evaluation framework was synthesised from a literature review and focus group. A fragment of the ten-page framework is provided in the Appendix. The framework is organised by Category, Characteristic and Criterion, and suggests a method for quantitatively assessing each criterion to enable comparisons between schemes, as well as a column for a user to document qualitative assessment. The rationale explains to users why a specific characteristic is important, while the criteria provide ways that the characteristics can be assessed. Four columns in the framework indicate the relevance of a criterion to the four key user types.

In constructing the preliminary framework, it emerged that the credibility of an IT security certification scheme is substantially linked to (1) the credibility of the organisation that issues it and (2) factors which relate more specifically to the certification. The existence of this relationship transfers the requirement for certification scheme rigor and transparency to the governing body for a given certification scheme. There has been validation of this point by the recently released ISO standard 17024, which specifically addresses this area.

The preliminary framework offers important advantages for users aiming to select an IT security certification scheme. By providing the criteria for assessing the characteristics and the rationale for their inclusion, it is possible for a user to better understand the relative importance of a particular criterion in their particular circumstances. In addition, by providing a standard set of criteria, it is possible to make a genuine comparison between certifications. A drawback of the framework in its current form is that weightings for each criterion to express individual preference for certain criteria are missing and this weakness reduces the level of customisation that is immediately available. A future development of the framework will include weightings with the aim of producing a scheme which would associate a numerical value with the relevance of a certification scheme to a particular group of security specialists.

4 Conclusion

A preliminary IT security certification evaluation framework has been developed in this paper. The framework is extensible and sufficiently flexible to allow different categories of users to identify those characteristics which are of greatest importance. Such flexibility will allow a user to make a more informed choice and will also allow customisation of the framework to individual user needs. Issues of governance emerged as significant contributors to the credibility of an IT Security Certification and this point has been underscored by both the recent trend to conformance with ISO 17024 by a number of schemes such as CISSP and CISM, and considerable feedback from the focus group participants. Future development of the framework will allow for the addition of user-defined weightings to be applied to each criterion together with a diagrammatic representation of the profile of each certification to allow for a greater level of comparison. A further focus group is planned to validate the final framework. The development of an automated tool to assist in evaluation and comparison presents another potentially useful direction to pursue.

References

1. M. Hentea, and H.S. Dhillon, Towards Changes in Information Security Education, *Journal of Information Technology Education* **5**, 221-223 (2006).
2. E. Tittel and K. Lindros, Analysis: The Vendor-neutral Security Certification Landscape, SearchSecurity.com, 26 September (2006).
3. APECTEL, IT Skills Report, Asia-Pacific Economic Cooperation Telecommunications & Information Working Group e-Security Task Group, (March 2004); http://www.apectelwg.org Document number: telwg29/ESTG/05.
4. E. Tittel, Building a Career in Information Security, *Certification Magazine* April (2004).
5. M. Bean, The Quest for the IT Security Professional, *Certification Magazine* November (2004).
6. E. Tittel, Security Certification: A Marketplace Overview, *Certification Magazine* February (2003).
7. M.E. Whitman, and H.J. Mattord, A Draft Model Curriculum for Programs of Study in Information Security and Assurance, Kennesaw State University, Georgia, 1 – 83 (2003).
8. M. Bishop and D. Frincke, Academic Degrees and Professional Certification, *IEEE Security & Privacy Magazine* November, **2**(6), 56 – 58 (2004).
9. K.L. Bledsoe and J.A. Graham, The Use of Multiple Evaluation Approaches in Program Evaluation, *American Journal of Evaluation* **26**(3), 302-319 (2005).
10. T. Claburn, Security Pros get their Due, *Information Week*, 16 January, (2006).
11. B. Endicott-Popovsky, Ethics and Teaching Information Assurance, *IEEE Security & Privacy Magazine*, July/August, 65-67 (2003).
12. T. Facklam, Certification of Persons – ISO/IEC DIS 17024, *ISO Bulletin* October, 31 – 34 (2002).
13. D. Frincke, Who Watches the Security Educators? *IEEE Security & Privacy Magazine*, May/June, 56 – 58 (2003).
14. P.Y. Logan and A. Clarkson, Teaching Students to Hack: Curriculum Issues in Information Security, ACM SIGCSE Bulletin, *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education SIGCSE '05* **37**(1), 157-161 (2005).
15. E. Schultz, Infosec Certification: Which way do we turn from here? *Computers & Security* **24**(8), 587-588 (2005).
16. ISO/IEC 17024, Conformity Assessment—General Requirements for Bodies Operating Certification of Persons, 1-10 (2003).

Appendix: Fragment of Preliminary Framework for User Evaluation of IT Security Certification Schemes

Legend: PRO - IT Security Professionals; EMP - Employers of IT Security Professionals
DEV - Developers of IT security courses; GOV - Governments

Categ-ory	Characteristic	Criterion	Rationale	PRO	EMP	DEV	GOV	Method of Quant. Assessment	Qualitative Assessment (user)
Credibility	Governance	With which Governance standards does the Certification Scheme conform? (e.g. ISO standard 17024)	If the governance of the organisation which is behind a particular IT security certification scheme is not open and transparent with few, if any, conflicts of interest, then the scheme is unlikely to attract the credibility necessary to be successful.	x	x	x	x	None = 0 At least one recognised standard = 1	