IT Security Certifications: Stakeholder Evaluation and Selection

Nicholas J.A. Tate
Faculty of Science and Technology
Deakin University
Burwood, Australia
Email: n.tate@its.uq.edu.au

Sharman Lichtenstein
Matthew J. Warren
School of Information Systems
Deakin University
Burwood, Australia
Email: sharman.lichtenstein@deakin.edu.au; matthew.warren@deakin.edu.au

Abstract

Information technology (IT) security certifications have proliferated in recent years. However they differ in regards to stakeholder considerations of credibility, accessibility and relevance. Key stakeholders with an interest in selecting an IT security certification (IT security professionals, employers, governments and higher education institutes) lack a systematic approach for differentiating between candidate certifications and selecting the "best" certification to satisfy requirements. The paper focuses on reporting a confirmatory focus group from a recent research project. It provides a framework for supporting stakeholder evaluation and selection of IT security certifications and discusses key implications for the IT security industry, IT security certifications, and the higher education sector.

Keywords

IT Security, IT Security Certification, IT Security Professional, Information Security, IT Certification

INTRODUCTION

Globally, and locally in Australia, there is an increasing organisational demand for skilled IT security professionals (Margolis 2008; Rossi 2007). An information technology (IT) security certification (hereon termed "security certification") is viewed by employers, governments and educators as an important qualification for IT security professionals (Armstrong & Armstrong, 2007; Hentea et al 2006; Vijayan 2007; Whitney 2007). This perception is also held in the local Australian context (where the study reported in this paper is located), as evidenced by the recent recognition of at least one security certification, CISSP, as part of the Federal government's migration process. In a recent global survey, 36 percent of employers were sending IT professionals to security certification courses to address the IT security skills shortage (Margolis, 2008). Indeed, IT security certifications are one of the few types of IT certification currently in demand (Marsan, 2007). Yet there are hundreds of security certifications available, presenting a challenge for IT security professionals, employers, higher education (HE) institute course developers and government agencies attempting to select the "best" security certification scheme to meet situational and individual requirements.

Recently experts have called for a single international IT security certification tied to a planned IT security Common Body of Knowledge (CBK) (e.g. Nance & Hay, 2007). Such a certification would replace the current proliferation of security certifications. However so far there has been little support for such consolidation, possibly due to the competitive value of the schemes for developers, ongoing competition between certification bodies, and diverse target markets for certifications; hence, new security certifications continue to appear (e.g. Sosunovas & Vasilecas 2007).

In this increasingly complex setting, how do IT security professionals and other stakeholders select a security certification that meets their special needs and context, from the current range available? Currently there is a lack of systematic approaches for selecting the "best" security certification. By September 2006, there were around 100 vendor-neutral security certifications and around 40 vendor-specific security certifications (Tittel & Lindros, 2006) suggesting that selecting the "best" certification is an onerous and *ad hoc* undertaking. Existing approaches to security certification evaluation are neither rigorous, systematic nor complete, and have often been constructed from a North American perspective. Some approaches allow comparisons of the skills and curriculum scope (e.g. SIFT 2008). However more generally, approaches do not consider wider and unique stakeholder needs in regards to certification *credibility*, *accessibility* and *relevance*.

This paper provides key findings from the final phase of a research project - a confirmatory focus group - and reports 1) a service-oriented framework for supporting stakeholder evaluation of IT security certifications, 2) a discussion of key stakeholder considerations, and 3) practical implications for the IT security industry, security certification developers and HE institutes. The framework is intended to support five key stakeholder groups – potential and experienced IT security professionals, employers, HE institutes and governments. It aims to provide services which assist a stakeholder in understanding and ranking the relative merits and positioning of each certification, thereby supporting certification selection.

The paper proceeds by providing a theoretical background developed from a review of relevant literature. Next, the research design is outlined. The paper then presents its key findings and concludes with a summary of key theoretical and practical implications.

THEORETICAL BACKGROUND

Key Stakeholders in IT Security Certification Evaluation and Selection

Four key stakeholder groups have a special interest in security certifications and selection of the “best” one. First, IT security professionals are interested in holding the “best” security certification for the purposes of employment, expertise development and increased remuneration (SIFT, 2008). Ott observed, referring to the different bodies that offer IT security certification, that “each of these organizations wants to be the premier independent certification, but how does an information security professional determine which one provides value-added credentials?” (Ott 2001, p2).

Second, a systematic IT security certification evaluation approach may assist HE institutes aiming to develop IT security courses that equip students for careers as IT security professionals. Experts recently argued for a role for IT security certification in HE information security courses (Armstrong & Armstrong, 2007). Yang (2001, pp237-238), in examining the impact of information security on computer science education, selected four programmes and attempted to identify common themes. However neither the range of schemes considered, nor the depth of analysis, would sufficiently inform a course designer about which scheme would be most appropriate to include in a particular degree. Meanwhile IT security course curricula are being standardised (Whitman & Mattord, 2003) without the benefit of knowledge of key differences and merits of various security certifications.

Third, employers seek IT security professionals with the most relevant security certifications. Many employers use security certifications during recruitment as a filter (Gross, 2003). Lainhart notes that employers are “relying on [IT security] certifications to identify prospective employees with experience and expertise” (Lainhart, 2008). As candidates may possess certifications from many different bodies, a security certification evaluation model would allow them to effectively compare a range of certification schemes with the requirements of their organisation. Lainhart also remarks that, particularly in the United States, holding the “right” certification has become especially important for organisations due to Sarbanes-Oxley regulation and increased security scrutiny worldwide.

Finally, a systematic approach to security certification evaluation could be useful to governments seeking to determine the relevance of particular qualifications for accelerated immigration purposes or for the purpose of regulating the IT security profession.

Categories, Characteristics and Criteria for Evaluating IT Security Certification Schemes

In the research project a security certification evaluation model was developed (as will be described in the Research Design section) which supports a systematic comparison of a set of IT security certifications. Eleven characteristics, grouped into three major categories, underpin the evaluation model (summarised in Table 1). The characteristics and categories were originally developed from a literature review and refined and extended during the project. Each characteristic has one or more evaluation criteria (summarised in Table 1) which are weighted by individual stakeholders and used during application of the model to assess the merits of each security certification. Further details of the categories, characteristics and evaluation criteria - and the application of the model to support certification evaluation, ranking and selection - can be found in Tate et al (2007b).

Table 1. IT Security Certification Evaluation Model:
Categories, Characteristics and Evaluation Criteria

CATEGORY	*CHARACTERISTIC*	*EVALUATION CRITERIA (CS = Certification Scheme)*
CREDIBILITY	Governance	- With which governance standards does the CS conform? (e.g. ISO standard 17024?) - Does the CS have a governing Board? - Is the CS independent of a training provider which may benefit from it commercially or otherwise? - Are the profits from the CS re-invested in it? - Is the CS able to operate without direct or indirect government control? - Does the governing board of the CS have members from more than one country? - Is the governing board of the CS able to act independently of the scheme owner?
	Assessment	- Does the CS use an open examination as a means of assessment? - If an examination is used, what are its characteristics? - What other assessment is undertaken?
	Curriculum Definition	- Is the CS based on a recognised body of knowledge which is published and publicly available? - Is the body of knowledge based on applicable standards such as those from ISO? - Is there a clear process for reviewing and updating the body of knowledge on a regular basis? - How often must candidates submit for re-certification?
ACCESSIBILITY	Access Restrictions	- Can the CS be obtained without a required training course from the offering body? - Does the CS require a mandatory training course?
	Cost	- What is the cost of attaining certification? - What is the cost of retaining certification?
	National Restrictions	- Are there any restrictions on access to the CS, based on nationality? - If training is mandatory before applying for certification, are there restrictions on access to the training, based on nationality?
RELEVANCE	Vendor Neutrality	- Is the CS run by a vendor to provide certification for its products?
	Academic Credentials and Experience	- Is a degree, or equivalent, an entry requirement for the CS? - How many years of information security work experience is required for the CS? - How is information security work experience verified?
	Ethical Code	- Does the CS have a professional code of ethics which all students who seek certification, must accept? - Have there been any cases where the ethical code has been enforced?
	Market Acceptance	- How many holders of certification from this CS are declared?
	Localisation	- Does the CS allow for local variation by jurisdiction? - Does the cost of the CS vary by country? - How many localised variants of the CS are available? - In what languages is the CS available? - In what countries is the CS offered?

Next we review existing literature supporting the inclusion of the *Credibility*, *Accessibility* and *Relevance* categories and related characteristics for evaluating security certifications, in the evaluation model. For a certification to be considered acceptable by a stakeholder it must first be perceived as *credible*. As Facklam (2002, p32) suggests, "Confidence in the respective certification schemes is achieved by means of a globally accepted process of assessment, subsequent surveillance and periodic re-assessments of the competence of certified persons". Three key characteristics of credibility are: *governance*, *assessment* and *curriculum definition*.

First, if the *governance* of an organisation that offers a particular security certification is not open and transparent – with few, if any, conflicts of interest – we argue that the scheme lacks credibility. In addition, if governance is not seen to guarantee certification independence from commercial, government or national interests, the scheme also lacks credibility. The importance of certification governance is illustrated by the proportion of the ISO/IEC 17024:2003 standard (ISO, 2003) devoted to the rules for scheme governing bodies. The US Department of Defence requires its personnel to have information assurance certification that is accredited by this standard (McNulty, 2005). Second, the credibility of a certification scheme is linked to its *assessment*. Schultz (2005) suggests that many schemes are too simplistic in their assessment requirements. Third, the IT security *curriculum definition* represents the body of IT security knowledge offered and is therefore an important credibility characteristic (Hentea, & Dhillon, 2006; Schultz, 2005). In particular, the curriculum definition should include discussion and assessment of technological, legal and ethical aspects of IT security (Endicott-Popovsky, 2003). It should be current and based on relevant international standards. It is also argued that if the curriculum is so narrowly defined as to be only applicable to people who live in Connecticut and can configure a particular router, how credible could it be? On the other hand, if a security certification has a curriculum that is so broadly defined that 95 percent of the world's population could pass it after reading a magazine article, the certification clearly lacks credibility.

The *accessibility* of a scheme is important for egalitarian reasons (Bledsoe & Graham 2005). Three key 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 exist when it is mandatory that a candidate for certification examination first undertake a particular training course, thereby increasing costs and imposing additional constraints. Second, stakeholder 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. Third, as cybersecurity becomes increasingly linked to national security, *national restrictions* may apply to the selection of candidates for IT security courses. Frincke (2003) observes that "Many security programs already segregate their audiences to a certain extent, for certain material … Some US agencies limit participation to those with US citizenship". Is it feasible to have a global IT Security certification scheme if selected aspects are limited to citizens of a particular country?

Certifications should be *relevant* to stakeholders. Five key characteristics of relevance are: *vendor neutrality, academic credentials and experience, ethical code, market acceptance* and *localisation.* First, regarding *vendor neutrality*, there are vendor-specific certifications which certify that the certification holder has knowledge of a vendor product and related skill sets. There are also vendor-neutral schemes which certify broad knowledge of a particular domain, that are generally run by an industry or "not-for-profit" group. Some of these schemes offer a range of certifications focusing on specialised skill sets – for example, GIAC (Pike, 2008). Second, regarding *academic credentials and experience*, key questions about a certification scheme are "What are its objectives?" and "How does the scheme relate to an academic degree in IT security?" Experts suggest that vendor-neutral certification is 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 practice in IT security, which would not normally be included in a degree. On the other hand, vendor-specific certification focuses on skills training for particular products. Third, with IT security, a *code of ethics* can assume particular importance since the knowledge needed to defend systems and networks against attack is the same knowledge that could be used to attack them (Logan & Clarkson 2005). 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 become irrelevant (Claburn 2006). Fifth, 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 where it operates. 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.

RESEARCH DESIGN

A research project was conceived to identify an approach for the systematic evaluation and selection of an IT security certification scheme for each of the four key stakeholder types (IT security professional, employer, government and HE institute). As the environment for IT security certification evaluation involves people, an interpretive research approach was adopted (Walsham 1995). The success or failure of an IT security certification evaluation is dependent on those who conduct the evaluation. We investigated the perceptions and experiences of the key stakeholder types in a four phase study.

In Phase One, a literature review was conducted to provide a theoretical background and establish research questions. The literature review also revealed only piecemeal approaches to the evaluation and selection of security certifications; these approaches did not systematically consider stakeholder requirements and preferences, and did not meet key objectives for such an approach (Tate et al, 2007a). Next, as discussed above, scholarly, professional and popular literatures in the information security domain were reviewed and synthesised to develop key categories and characteristics for a draft evaluation model.

In Phase Two, the draft evaluation model was explored by a two hour focus group session at the AusCERT2006 conference held on the Gold Coast, Australia, in May 2006. The focus group participants comprised seven senior IT security representatives from industry, HE institutes and national government agencies. Two participants are international experts in information security. Three participants are IT security professionals at Australian and New Zealand Universities. The sixth participant is an IT security specialist with a government department, and the remaining participant is the director of IT Security engineering for a major IT vendor. The session was moderated by a senior Australian academic in information security. The focus group session debated significant issues relating to the draft model. Notes and a session transcript were analysed for key themes using successive iterations of inductive qualitative content analysis (Mayring 2000). Findings supported the draft model and also suggested several enhancements. The researcher also further explored the themes that suggested criteria for assessing the framework's characteristics, by a literature review and an examination of ten security certifications. He was thus able to develop evaluation criteria for each characteristic in the model, rationale for the criteria, and stakeholder relevance for each criterion. A revised evaluation model was produced incorporating all findings.

In Phase Three the revised evaluation model was trialled by the first author – a senior IT Security Professional – by applying the model (initially implemented as an Excel spreadsheet) to three IT security certification schemes. The aim of the phase was to discover flaws in the model and identify improvements. Key findings from the first three phases were provided in Tate et al (2007a, 2007b) and included further enhancements.

In Phase Four, the revised evaluation model (from Phase 3) was confirmed by a two hour focus group session held at the Educause Australasia 2007 conference in Melbourne, Australia, in April 2007. The focus group participants comprised seven IT security representatives from the IT industry, HE institutes and Australian government agencies. The first two participants had been involved in implementing an internal IT security certification scheme for a major international consultancy. They are a senior IT security professional, and a senior IT security manager for the Asia-Pacific region. The third participant manages IT infrastructure, including IT security, at a major Australian university. He has also participated in national IT security initiatives within the university sector. The fourth and fifth participants are senior managers at different international IT vendors. One has experience in IT security design and consultancy for a major systems vendor and was at the time a technical manager. The other was employed at a major network vendor as a Systems Engineer, and is experienced in IT security engineering and, in general, IT certification. The remaining two participants are in their twenties; they have recent university study experience, one was completing a doctorate in information security management at an Australian university; and the other was a recent graduate of an information systems undergraduate degree (which included a final year information security unit), who had attended an Australian university as an international student.

The session was moderated by a senior Australian academic in information security. The focus group session debated significant issues relating to the revised evaluation model. Notes and the session transcript were analysed for key themes using iterations of inductive qualitative content analysis (Mayring 2000). Findings confirmed the revised evaluation model (summarised in Table 1) and enabled development of a contextual operational framework for offering the model (Figure 1 in the next section.). Further themes were grouped into findings that are also reported in the next section, with fictitious company names employed to preserve confidentiality.

FINDINGS

Support for IT security certification evaluation model

The evaluation model (summarised in Table 1) was strongly supported by all participants. First, the category of "Credibility" was well supported. One participant suggested that the credibility of a security certification is linked to the information security standard which the certification follows, but that such standards often lack currency. Therefore if security standards are used as the exclusive basis for a security certification's curriculum, there is a strong likelihood that the certification's content will lack currency. There was also agreement that the assessment approach of a security certification plays a key part in its credibility:

> "We have our own [IT security] certification… and even though it is vendor-specific, the assessment is regarded as particularly tough … they really go out of their way to make life miserable for you in terms of the toughness of the assessment." [Systems Engineer, IT Network Vendor].
>
> "But is that important?" [Moderator]
>
> "Absolutely, it sorts out those that can, and those that can't. I've known people that have done it [the assessment] eight or nine times and failed it." [Systems Engineer, IT Network Vendor].

This participant also noted that certification assessment methods must prevent cheating via rapid dissemination of an exam over the internet. Without such a guarantee, a certification would have limited credibility.

When discussing the Curriculum Development characteristic (Table 1), participants noted the importance of basing a certification on a publicly available recognised CBK, supporting recent arguments (Nance & Hay 2007; Theoharidou & Grtiazalis 2007). A graduate noted the importance of wide-ranging coverage of any existing CBK for an IT security certification:

> "As a graduate, I'd like to do a scheme that incorporates a vast knowledge of security more broadly, rather than, for example, a vendor-based scheme, where it always feels as if you're tying yourself down to that product." [Information security PhD Student, BigOzUni].

One participant expressed concern that a security certification's curriculum often does not support employee specialisation in future job roles. He cited the example of "business continuity" which is a softer security skill, suggesting that it should be catered for in-depth by a security certification.

All participants agreed that *Accessibility* would be an important consideration when selecting a security certification. They argued that IT security professionals should be able to undertake an exam without training. Indeed, one graduate believed it a significant advantage to be able to access a certification exam without undertaking training. The discussion in the focus group centred on whether a certification should mandate a training course before allowing assessment. It emerged that some certifications require mandatory training from the certification provider. Such a mandate could raise the suspicion that the providers are using the schemes to generate income for training activities. Any mandated training, whether from the scheme provider or not, can therefore be viewed as an access restriction.

However both graduate participants saw cost as the key characteristic for evaluating the accessibility of a security certification. The international graduate commented that after paying hefty international student fees, it was important to keep costs down in future studies. At the same time, he observed that in several years' time, after saving from paid work, he may be prepared to pay high fees to complete a security certification.

Regarding *Relevance*, participants agreed that a security certification should be relevant and that the characteristics for relevance in the evaluation model are important. One vendor-employed participant was concerned that the presence of vendor-neutrality in the evaluation model implied that vendor-specific certifications were assumed inferior to vendor-neutral schemes. The participant's concern suggests a need for clarifying documentation to support the evaluation model. Interestingly, the two young graduates did not understand why vendor-neutrality may be important to the relevance of a certification, again suggesting a need for clarifying documentation. Some discussion took place on the differences between vendor-neutral and vendor-specific schemes and, in particular, on the broader perspective and greater longevity offered by vendor-neutral schemes. Participants expressed the view that such schemes were more like university courses whereas vendor-specific schemes had more characteristics in common with training courses. Some participants believed that IT security professionals should hold both types of certifications. Overall there was general support for the vendor-neutral characteristic. Finally it was disappointing to learn that the two graduate participants were not particularly concerned regarding whether a Code of Ethics was addressed by a certification scheme.

The value of the evaluation model was believed to be broader than its intended use for IT security certification evaluation and selection. For example, one participant remarked:

> "Personally, I find all of the information [offered by the evaluation model] extremely useful because on top of what I'm doing, I'm also part of the ISACA Education and Training committee and that's looking at how we sell the cycle of certification to new members and what will attract them to come in and do that certification.." [Security Professional, WorldITConsult].

Another participant suggested a further marketing use for the model:

> "So being able to pull all this information together and give it to graduates or experienced [IT Security] professionals and say 'this certification has completed 90 percent of all of these criteria from an independent study or independent framework'. You know that might encourage people, instead of saying, 'well, you know, we really think that it's important'". [Security Professional, WorldITConsult].

Still another participant identified the model as an excellent new perspective on security certifications and indicated that it would be useful to him personally.

> "I feel empowered as a consumer of certification services in a way that I didn't actually realise until we had this exercise [the focus group]. I think really taking this [evaluation model] in and using this as a tool for you to go out and help educate yourself - this is powerful stuff! And also for myself being a lifelong learner, I'm going to use this. And I think this is a generally acceptable way of looking at certifications." [Information Security Manager, World IT Consult].

Implementation of Security Certification Evaluation as a Service

It was explained to focus group participants that input to the evaluation model when applied would comprise: 1) objective data about each security certification (e.g. details about the governance of a security certification); and 2) subjective weightings reflecting stakeholder priorities. Participants suggested the possibility of streamlining the process of comparing and assessing IT security certification schemes, by delegating the task of collecting the data to a trusted entity which will undertake this collection once on behalf of all stakeholders. If potential users of the evaluation model can be persuaded to trust a hosted version, which has been pre-populated with objective data from all the certification schemes, an individual user need only provide a set of weightings which reflects their own circumstances and preferences.

Participants strongly agreed that the objective collection of data, population of the framework and hosting of the online tool to support the framework should be undertaken by a trusted, independent body such as the CERT bodies – in Australia, that is AusCERT:

> "I wouldn't want this to be held in an ISACA or ISC2 because I think then people won't see the neutrality of it. They might see it as just another way to sell a certification. I would like it be in a constant independent body which is basically just educational. And I think that's what AusCERT is." [IT security professional, WorldITConsult].

Other potentially valuable suggestions from participants have significant implications beyond the scope of the research project. They will be the subject of future research and maintenance of the evaluation model, and include:

- extending the evaluation model to record employer ratings of schemes;
- populating the evaluation model with data from all security certifications;
- producing a brochure to accompany the evaluation model; and
- extending the evaluation model to highlight salary levels for particular security certifications.

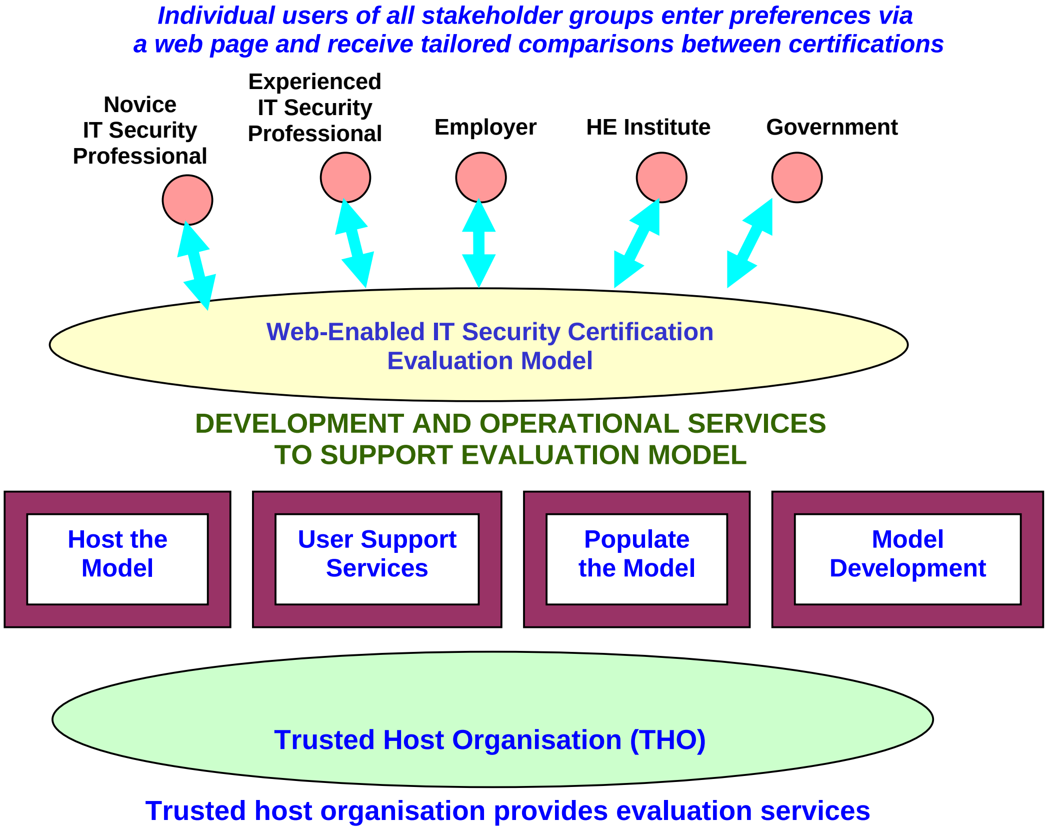
Individual users of all stakeholder groups enter preferences via
a web page and receive tailored comparisons between certifications
Novice IT Security Professional
Experienced IT Security Professional
Employer
HE Institute
Government
Web-Enabled IT Security Certification Evaluation Model
DEVELOPMENT AND OPERATIONAL SERVICES TO SUPPORT EVALUATION MODEL
Host the Model
User Support Services
Populate the Model
Model Development
Trusted Host Organisation (THO)
Trusted host organisation provides evaluation services

Figure 1: Framework for Stakeholder Evaluation of IT Security Certifications

A service-oriented Framework for Evaluating IT Security Certification Schemes (Figure 1) emerged from the focus group findings and was subsequently developed in detail. According to this framework, a Trusted Hosting Organisation (THO) will develop, maintain and offer a web-enabled application which implements the evaluation model. The THO will host the evaluation model and enable access by individual users across the internet. The THO will also provide support services such as published lists of Frequently Asked Questions (FAQs), application maintenance (bug fixing) and end-user help facilities.

In summary, it is anticipated that the Trusted Hosting Organisation (THO) would need to develop an application to implement the evaluation model and provide four operational and development services to support the application:

- hosting service to host the application;

- support services for application users;
- data population service to keep the application up to date;
- development service to undertake future development of the application.

DISCUSSION

A key finding is that THOs such as AusCERT - and other CERT agencies worldwide - could provide certification evaluation and related services as shown in Figure 1. Key advantages of the service-oriented framework (Figure 1) include allowing users to use the evaluation model without undertaking their own market research. The THO would regularly research the security certification market and populate the application with both general market data and data on currently available IT Security certification schemes. This pre-population of the application means that all previously defined "objective" data for the model would be immediately available for end-users. This has the dual benefit of facilitating a genuinely objective collection of data while relieving each potential user of the burden of data collection. For the model to remain useful, however, it is likely that the THO would need to undertake further development to address changes in market and user expectations. It remains to be seen, of course, whether AusCERT could and would host the application and offer related services. AusCERT and other CERTs are used to securely hosting a range of services so it is likely that they would have the requisite capabilities.

A key disadvantage of the framework is its resourcing implications. For example, the cost of collecting the data would be borne by the hosting organisation and is likely to be costly**.** For AusCERT to be willing to host the framework may mean that some level of government funding is made available. Indeed, participants in the focus group strongly believed that governments should support THOs in hosting the application and related services by providing adequate resources, and that they should therefore be approached for sponsorship. Indeed the key barrier identified to the implementation of the evaluation model was existing lack of support from governments. One participant expressed surprise that the Australian government was not already undertaking this sort of activity because it relied upon security certifications for assessing visa applications from IT security professionals. Surprisingly, although the Australian Government commissioned a report on IT security certifications from a consultancy (SIFT 2005), it concluded that no Australian certification was needed to satisfy the national context, and did not recommend any mechanism for helping Australian IT security professionals make choices between available international certifications. Since then, however, an APEC sponsored web site has been established which enables comparisons between certifications based on curriculum coverage (SIFT 2008). Clearly the findings from this paper suggest that much more is needed and government support will be sought accordingly.

Another key finding concerns the quality of education of IT security professionals. First, participants emphasised that in Australia, employers are experiencing a shortage of knowledgeable skilled IT security personnel. New graduates from HE institutes lack the right combination of breadth and depth of security knowledge needed by IT security professionals working in specialised security roles. Furthermore, it was mentioned in the focus group that HE institutes, by removing most if not all prerequisites from units, and enrolling students with diverse backgrounds (some with work experience, others with none) in units, effectively limit IT security graduate achievements in the workplace. To partly address this issue, HE institutes should aim to ensure that IT security graduates achieve highly in their studies. Given the limitations of current HE program models, complementary security certification and training are recommended for IT security graduates. However, IT graduates planning to work as IT security professionals should be advised first to work in the IT security field for several years before undertaking IT security certifications. This recommendation is important because IT graduates are likely to find it challenging to select appropriate weightings for different security certification characteristics without the background that only experience can provide. The recommendation to work for several years post-graduation is further supported by the lack of awareness displayed by the two IT security graduates in the focus group, with regard to important certification characteristics such as Governance and Assessment.

The focus group findings further suggest that many IT security certifications lack a balance of breadth and depth in their curriculum. First, it is not enough to only teach security technology as management issues and process issues (eg business continuity) are increasingly valued in the workplace. The need for IT security professionals to possess information security management skills is supported by recent evidence of strong demand for business continuity certifications based on the new BS25999 standard (Ashford 2007). Second, vendor-specific certification schemes traditionally lack breadth while vendor-neutral schemes frequently lack depth. The focus group findings suggest that vendor-specific and vendor-neutral schemes could be combined in a complementary way to provide both breadth and depth, although the cost of undertaking two courses may be prohibitive. Other possibilities include designing new security certifications that allow for a general core and specialisation. The need for breadth and depth in security certifications is clearly an issue for IT security certification developers and HE institutes to address.

Regarding security certification currency, IT security certification schemes require a level of risk-taking by IT security professionals as it cannot be known in advance whether a particular certification has longevity. Each certification should be governed by a body which ensures renewal to partly mitigate this risk. Yet many certifications are unable to stay current due to slow-moving standards. This challenge for standards should be investigated in future research.

The key access barrier to security certifications, as identified by the focus group, is cost. While evidence supporting this conclusion was obtained from only two graduates, if this issue exists on a wider scale it will contribute to the current shortage of IT security professionals. As mentioned above, there was support from the focus group for the suggestion that IT graduates should aim to work in the field for several years before undertaking an IT security certification scheme; such a strategy would provide savings toward certification fees. Some employers also sponsor employees to undertake security certification, which will help alleviate cost concerns; this practice should be encouraged by governments.

Nance and Hay (2007) have proposed the consolidation of current IT security certifications into one international IT security certification. While the focus group did not suggest such a consolidation, which may reduce the opportunities afforded by current certifications, there should be wider debate in relevant communities about the future direction of IT security certifications in order to avoid continued proliferation and related challenges in stakeholder evaluation and selection.

CONCLUSION

This paper has reported findings from a confirmatory focus group which was the final phase of a large research project investigating an approach to evaluate and select an IT security certification scheme. Key theoretical findings included an evaluation model (summarised in Table 1) and a service-oriented framework (Figure 1) depicting the hosting of evaluation and related services by a trusted host organisation. The paper also provided theoretical insights to add to existing theory on IT security certification, and practical recommendations for key stakeholder groups (IT security professionals (novices and experienced), employers, governments, certification developers and HE institutes). When implemented, the framework will contribute to improved IT security in organisations. Additional benefits may be obtainable by applying the framework in conjunction with complementary tools (e.g SIFT, 2008, which addresses the scope of a certification).

Key themes emerging from the paper are the need for 1) improvements in IT security certifications in terms of currency of content and currency of standards which are slow moving due to lack of resources and competing interests; 2) greater interest and support from governments; 3) improved IT security education at HE institutes; and 4) a need for greater awareness by IT security graduates of the key issues surrounding and differentiating IT security certifications. Once again, it is surprising that, given the general trend of developed societies to increase consumer choice through improved access to information, there has been no evidence of any government initiative to sustainably support IT security professionals in this direction. Finally, an overarching theme emerging from the research is that IT security certification consumers of all kinds can be empowered by the framework and evaluation model produced in the research project and discussed in this paper. Future research should aim to extend the work carried out to date as suggested in the paper, with the intention of providing greater consumer empowerment while improving information security in organisations globally.

REFERENCES

ISO 2003. ISO/IEC 17024:2003: Conformity Assessment - General requirements for bodies operating certification of persons”, International Organization for Standardization, pp. 1-10.

Armstrong, H. and Armstrong. C 2007. “The Role of Information Security Industry Training and Accreditation in Tertiary Education”, in IFIP International Federation for Information Processing, Vol 237, Fifth World Conference on Information Security Education, eds. Futcher, L., Dodge, R., (Boston: Springer), pp. 137–140.

Ashford, W. 2007. “Irwin Mitchell aims for BS25999 business continuity certification”, *Computer Weekly.com*, November 2.

Bledsoe, K.L. and Graham, J.A. 2005. “The Use of Multiple Evaluation Approaches in Program Evaluation”, *American Journal of Evaluation*, 26(3), pp. 302-319.

Claburn, T. 2006. “Security Pros get their Due”, *Information Week*, 16 January, p. 78.

Endicott-Popovsky, B. 2003. “Ethics and Teaching Information Assurance”, *IEEE Security & Privacy*, Jul/Aug, pp. 65 – 67.

Facklam, T. 2002. “Certification of Persons – ISO/IEC DIS 17024”, *ISO Bulletin*, October, pp. 31 – 34.

Frincke, D. 2003. “Who Watches the Security Educators?” *IEEE Security & Privacy*, May/June, pp. 56 – 58.

Gross, G. 2003. “Employers Want Security Certifications”, *Network World*, 5th November 2003, Retrieved 28 September, 2008, from http://www.networkworld.com/news/2003/1105seccert.html?page=1

Hentea, M., Dhillon, H.S. and Dhillon, M. 2006. ”Towards Changes in Information Security Education”, *Journal of Information Technology Education*, 5, pp. 221-223.

Lainhart, J. 2008. “Certification Proves Its Worth to IT Security Professionals and Employers”, GoCertify.com, 6th February 2008, Retrieved 28 September 2008 from: http://gocertify.com/article/ISACA-Certifications1.shtml

Logan, P.Y. and Clarkson, A. 2005. “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), pp. 157-161.

Margolis, G. 2008. “Survey Indicates Gap Between IT Security Skills’ Supply and Demand”, *Certification Magazine*, March 3.

Marsan, C.D. 2007. “Which certifications are worth your time?” *Network World*, 27 November.

Mayring, P. 2000. “Qualitative Content Analysis”, *Qualitative Social Research Forum,* 1(2), Retrieved 28 September 2008 from: http://www.qualitative-research.net/fqs-texte/2-00/2-00mayring-e.htm

McNulty, L. 2005. “Preparing for Implementation: Professional Certification under DOD Directive 8570.1”, in *Proceedings of Military Communications Conference 2005 (MILCOM 2005*), IEEE, 3, pp.1485- 1487.

Nance, K. and Hay, B. 2007. “Certifying the Computer Security Professional Using the Project Management Institute's PMP Model”, in *New Approaches for Security, Privacy and Trust in Complex Environments*, IFIP International Federation for Information Processing, Volume 232, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer), pp. 491–496.

Ott, J. L. 2001. “The State of Our Profession”, *Information Security Systems*, May/June, pp. 2 – 4.

Pike, J. 2008. “GIAC: The Hands-On IT Security Certification”, *Certification Magazine*, June.

Rossi, S. 2007. “Skills shortage set to restrict Australia's ICT growth in the long term”, *Computerworld.com*, Retrieved 28 September 2008 from: http://www.arnnet.com.au/index.php/id;1724064896

Schultz, E. 2005. “Infosec Certification: Which way do we turn from here?” *Computers & Security,* 24(8), pp. 587-588.

SIFT 2005. “Information Security Skills Accreditation in Australia – The Current State and Industry Consensus on the Way Forward”, *SIFT Information Security Services*, November, pp 1-98.

SIFT 2008. “APEC (Asia-Pacific Economic Cooperation) Guide to Information Security Skills: Matching Certifications to your Business or Career”, SIFT Pty Ltd, Australia.

Sosunovas, S. and Vasilecas, O. 2007. “Four security certification levels for IT Managers and Staff in the Public Sector”, in *Proceedings of the International Conference on Emerging Security Information, Systems, and Technologies(SecurWare 2007),* pp 7-11, Valencia, Spain.

Tate, N., Lichtenstein, S. and Warren, M.J. 2007a. “Toward User Evaluation of IT Security Certification Schemes: A Preliminary Framework” 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, 1., von Solms, R., (Boston: Springer), pp. 473–478.

Tate, N., Lichtenstein, S. and Warren, M.J. 2007b. “Supporting User Evaluation of IT Security Certification Schemes”, in *Proceedings of Eighteenth Australasian Conference on Information Systems (ACIS 2007*), Toowoomba, Queensland.

Theoharidou, M. and Grtiazalis, D. 2007. “Common Body of Knowledge for Information Security”, *IEEE Security & Privacy,* 5(2), pp. 64-67.

Tittel, E. & Lindros, K. 2006. Analysis: The Vendor-neutral Security Certification Landscape, SearchSecurity.com, 26 September, Retrieved 28 September 2008 from: SearchSecurity.com.

Vijayan, J. 2007. Salary premiums for security certifications increasing, study shows, *Computerworld*, 9th July.

Yang, A. 2001. Computer Security and Impact on Computer Science Education, *The Journal of Computing in Small Colleges (JCSC), 16*, 4, pp. 233-246.

Walsham, G. 1995. “The Emergence of Interpretivism in IS Research”, *Information Systems Research*, *6*(4), pp. 376-394.

Whitman, M. E. and Mattord, H. J. 2003. A Draft Model Curriculum for Programs of Study in Information Security and Assurance, Kennesaw State University, pp. 1 – 83.

Whitney, K. 2007. The International Market for Certification, *Certification Magazine*, May.

COPYRIGHT