Certifying the Computer Security Professional Using the Project Management Institute's PMP Model

Kara L. Nance and Brian Hay
ASSERT Center, University of Alaska Fairbanks
210 Chapman, Fairbanks, AK 99708 U.S.A.
ffkln@uaf.edu brian.hay@uaf.edu
WWW home page: http://assert.uaf.edu

Abstract. While many organizations offer certifications associated with information technology (IT) security, there is no single overarching accrediting organization that has identified the body of knowledge and experience necessary for success in the IT security field. In order for an IT security workforce to be acknowledged and recognized throughout the world as possessing a proven level of education, knowledge, and experience in IT security, a formal process for certifying IT security professionals must be developed. This research effort suggests that the IT security community use the Project Management Institute's process for certifying Project Management Professionals (PMPs) as a model for developing an open and easily accessible IT Security Body Of Knowledge (ITSBOK) and an associated international certification process for IT security professionals.

1 Introduction

Information security has become an increasingly important issue, and the repercussions of a failure in information security have become much more serious as the level of public, corporate, and governmental awareness of such issues has been raised. Twenty years ago the loss of bank backup tapes or university student records may not even have been reported to law enforcement agencies, whereas today such losses not only have legal implications, but are likely to be publicized by national news organizations. As such, the need for excellence in IT security is apparent not only within the IT community, but at all levels of the corporate and governmental hierarchies. The problem, however, is there currently is no suitable, vendor-neutral, standard by which to judge the competence of a potential IT security employee. While there are many certifications related to the information security field, many

have such a narrow or vendor-specific focus that they have little value in determining how an employee could adapt to new threats and technologies in this rapidly developing field. In many cases, IT security professionals have simply evolved into their current roles, often because they were system administrators who realized there was a need to "secure" the systems they were responsible for. However, when an individual evolves into such a position, the full breadth of information assurance issues is often missed, and is replaced by a focus on the threats that the employee in question is either aware of or can imagine. In addition, one need not search long to find any number of ill-conceived IT security plans, such as many of the current digital rights management (DRM) schemes, which most truly competent information assurance professionals know are doomed to failure. As IT security becomes increasingly important in all aspects of life, including those, such as RFID embedding in passports, which are not within the realm of traditional computer security, there must be a mechanism by which those truly qualified to design, implement, and manage such systems can be identified. In addition, there must be a roadmap for those without the in-depth experience or a wide ranging understanding of the information security discipline, including students, to develop throughout their careers into the IT security leaders of the future.

2 Background

In order to assess the training and certification needs of the computer security professional, one first must determine the background of the personnel who tend to hold security positions in IT fields. The rapid technological advances of the information age have resulted in a large number of IT workers who have evolved into their positions as well as those who have been trained for their positions. In many cases, the individual at the organization who knew the most about computers became the system administrator, without any formal training in system administration or computer security. In other cases, system administrators have a strong background in general computer science, but not specific training in computer security. ABET, Inc., the recognized accreditor for college and university programs in applied science, computing, engineering, and technology [1] does not currently include computer security as a required topic in a computer science or information technology curriculum.

To address the lack of trained computer security professionals, the National Security Agency (NSA) developed the Center of Academic Excellence in Information Assurance Education (CAE) program in response to Presidential Decision Directive 63 [2], with the goal of increasing the number of graduates with experience in information assurance. As of February 2003, the CAEIAE program is co-sponsored by the NSA and the Department of Homeland Security (DHS) [3]. There are currently approximately 70 academic institutions from across the United States that currently hold the CAE designation. This credential is intended to indicate that the institution is capable of producing graduates who have some minimal information assurance skills upon entry into the workforce. This is based on the national standards set by the Committee on National Security Systems and

indicates that the institution has mapped its courses to the NSTISSI standards such as 4011 [4].

There are, however, weaknesses associated with the current CAE model. One weakness is that the depth to which the topics are covered varies greatly across the certified programs. Another is the lack of mandatory association between the course mapping process and the IA certification process, given that there is no requirement in the CAE application process to demonstrate that students receiving IA certification have completed a comprehensive set of the courses mapped to a particular NSTISSI. While CAE institutions have been successful in raising the level of security awareness among students, nothing in this process addresses the continued development of skills beyond the academic setting, which is necessary to transition from the level of college graduate to that of a well-rounded, highly experienced IT security practitioner. While there are certainly many other bodies who currently offer various levels of security certification [10, 11, 12], the lack of standardization across this wide field is readily apparent as each responds to the needs of its identified target audience. Many, if not all, of the courses currently available were developed by the training organizations without conducting an industry-wide needs assessment, resulting in certifications which tend to target specific or current products and issues, rather than those which address the long term or higher level needs of the IT community.

IT is such a rapidly changing field that vendor or product-specific skills acquired in such courses either quickly become obsolete, or serve as a method by which organizations become dependant on specific vendors, simply because the costs involved in retraining for alternate products is prohibitively high in the short term. Thus it is important that certified professionals possess the underlying foundational knowledge necessary to allow them to adapt to the wide range of IT security threats that they are likely to encounter now, as well those future threats that have not yet been imagined. Crowley conducted a survey of current literature discussing information systems security training and education in industry, government and academia. [13] There is a clear lack of standardization across the many self-designated bodies that have chosen to offer certifications in computer security. The result is that the IT security community has not identified a dominant standards organization with an open and easily accessible body of knowledge to certify professionals in IT security.

3 PMI Model

3.1 Problem Description

The challenges regarding standardizing IT security professionals are very similar to the challenges that were successfully addressed in certifying project management professionals. The Project Management Institute is an international organization that has identified five process areas and nine knowledge areas as well as metrics for certifying individuals as Project Management Professionals (PMPs). The program administers a “globally recognized, rigorous, education, and/or professional experience and examination-based professional credentialing program that maintains

an ISO 9001 certification in Quality Management Systems."[5] Certified Project Management Professionals have demonstrated that they have met the education and/or professional experience requirements; have passed the rigorous PMP examination, have agreed to follow the PMP Code of Professional Conduct; and have committed to maintaining their status through continuing certification requirements. [6]

3.2 PMBOK

In addition to professional magazines, a refereed journal, and monthly newsletter, the Project Management Institute publishes A Guide to the Project Management Body of Knowledge (PMBOK Guide) [7]. This publication is currently in its third edition and has been translated into numerous languages to allow standardization of the field of project management across cultural and language barriers. The PMBOK was developed twenty years ago by PMI volunteers through a substantial research project, who worked together to identify the project management body of knowledge. [8] It is updated on a four-year cycle to ensure that it continually reflects the current state of the art in project management, based on input from its readers, and other project management professionals.

3.3 Experiential Requirement

The option to achieve the requisite training either through a bachelor's degree combined with some verified experience (>4,500 hours) or through more substantial verified experience (>7,500 hours) provides an excellent mechanism that opens the certification opportunity to those who have evolved into their positions in addition to those who have specifically been trained into the position. Both paths require experience so that the individual has proven themselves as a competent project manager. In addition, both tracks require at least 35 contact hours of formal education in project management. This experiential requirement would not be sufficient for certification on its own as this requirement would not provide a consistent measure of experience for all candidates nor ensure that the individual demonstrate comprehension of the body of knowledge necessary for success in the field. PMP candidates must complete an extensive application to verify that their background is consistent with the PMP eligibility requirements. Once approved, eligible candidates have one year to take the PMP examination. [9]

3.4 Examination

The four hour examination consists of questions that have been developed and validated by global work groups of experts in the content; each is referenced to at least one project management publication; they are monitored through psychometric analysis; and they satisfy the test specifications of a job analysis. [6] In addition, the breakdown for the exam topics is consistent with the performance domains. The examination is available in 10 languages and is offered only through approved test

centers under a very strict examination process. Passing the examination is the final step in becoming a certified Project Management Professional, although keeping the certification current requires a commitment to meeting the continuing education requirements to keep current in the field.

4 IT Security Solution

IT Security professional could be certified using a similar process, building on the success of the PMP certification process and adopting their model. To oversee this effort, an organization similar to the PMI would need to take leadership in the effort. A similar approach has been used by the International Information Systems Security Certification Consortium for Certified Information Systems Security Professional (CISSP), but the related body of knowledge and the test which covers the CBK, has been criticized as demonstrating only lower levels of Bloom's taxonomy of educational objectives rather than true understanding of the underlying concepts necessary for success in the IT security field. One of the first objectives for this organization would be to develop a concise Guide to the IT Security Body of Knowledge (ITSBOK). Similar to the PMBOK, this publication would be easily available and vendor-neutral, and could easily build on the existing NSTISSI standards.

A poll of IT security professionals could help determine the experiential components that would be required in order for individuals to be eligible for the certification. Much of this work has been done, especially through the identification of the formal requirements for an institution to be certified as a CAEIAE. Like the PMP content, the content would need to be presented in a consistent, evolutionary, and vendor-neutral format, with sufficient depth to guarantee mastery of content rather than mere memorization of facts. The criteria could be reevaluated in compliance with a set revision schedule to ensure that it continually reflected a consensus body of knowledge that was evident of best practices in the field of IT security. An examination over the content should be a mandatory component in the certification process in order to ensure that all certified individuals demonstrated competence in the IT security body of knowledge. Like the PMP candidates, an ITSP should be prequalified based on a combination of education, verified experience, and IT security training prior to becoming eligible to take the examination.

While the ITSBOK would form the basis for the ITSP certification process, it could also be used as a guide for the development of training programs, such as those offered by technical colleges, or internal corporate training programs. While these programs may or may not culminate in ITSP certification, they can still benefit from the clear designation of the goals defined in the ITSBOK. This approach would enable a scaleable solution to meet the needs of government, industry and academia.

5 Conclusion

To create a certification in IT Security that is accepted internationally is a lofty, but necessary and worthwhile goal. In order to accomplish this, an accrediting body must be identified or established, the IT Security Body of Knowledge must be defined, and the formal process for certification must be developed and published. The creation of an Information Technology Security Professional (ITSP) certification following the highly successful model of the Project Management Institute's Project Management Professional (PMP) certification would guarantee that the IT security arena would have a population that would be widely recognized and accepted throughout the world as possessing a proven level of education, knowledge and experience in IT security.

References

1. ABET. Retrieved November 1, 2006 from www.abet.org
2. Department of Justice. White Paper - The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. May 22, 1998. Retrieved November 1, 2006 from http://www.usdoj.gov/criminal/cybercrime/white_pr.htm
3. National Security Agency. Centers of Academic Excellence. Retrieved November 1, 2006 from http://www.nsa.gov/ia/academia/caeiae.cfm
4. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (INFOSEC) Professionals. NSTISSI No. 4011 20 June 1994.
5. Project Management Institute. PMI Home Page Retrieved November 1, 2006 from www.pmi.org
6. Project Management Institute. PMI Certification Program. Retrieved November 1, 2006 from http://www.pmi.org/info/PDC_CertificationsOverview.asp
7. Project Management Institute. A Guide to the Project Management Body of Knowledge – Third Edition. 2005.
8. Project Management Institute. Book Descriptions. Retrieved November 1, 2006 from http://www.pmibookstore.org/PMIBookStore/productDetails.aspx?itemID=358&varID=1
9. Project Management Institute. PMP Credential Handbook. PMI. 2000.
10. SANS Institute. Retrieved November 1, 2006 from http://www.sans.org/training/
11. ICS^2 Retrieved November 1, 2006 from https://www.isc2.org/cgi-bin/index.cgi
12. Global Information Assurance Certification. Retrieved November 1, 2006 from http://www.giac.org/
13. Crowley, E. 2003. Information system security curricula development. In Proceedings of the 4th Conference on information Technology Curriculum (Lafayette, Indiana, USA, October 16 - 18, 2003). CITC4 '03. ACM Press, New York, NY, 249-255.