Proceedings of the 11th Colloquium for Information Systems Security Education
Boston University
Boston, MA June 4-7, 2007

Professionalizing the Practice of Information Security

William H. Murray Naval Post Graduate School, Corey D. Schou, Idaho State University,
W. Vic Maconachy, Department of Defense [1]

Abstract – This paper describes aspirations for the information system security profession and steps for advancing them. It is about what the profession would look like if the authors and their associates could have it any way they wanted it to be. It describes a strategic vision. We do not expect this vision to be realized by accident. However, we believe that it can be achieved by design and intent within a decade. We make recommendations for meeting the requirements and challenge The Colloquium to lead the education component.

Index terms – Security; Professionalizing; Curriculum Certification

I. Aspirations for Our Profession

> If the sick are to reap the full benefit of recent progress in medicine, a more uniformly arduous and expensive medical education is demanded.—Abraham Flexner [2]

We must demand the same uniformity in the computer security profession if we are to reap the full benefit of a net-centric information based economy.

Ultimately, we would like the profession to be **recognized**, understood, appreciated, and respected. Said another way, when our dinner partner asks us what we do for a living, we would like to say that we are information system security professionals and have it mean something. While it might not mean the same thing as saying that we are doctors or lawyers, it should rank with accountant or auditor.

As a context for professional practice, we would like our profession and our colleagues to be **educated**. We would like them to have a liberal education, to appreciate literature, history, geography, art, science, mathematics, politics, economics, and government. We would like them to have a professional education characterized by completion of rigorous courses in the field. We want them to be articulate, to be masters of spoken and written communication. We would expect this education to manifest itself in appropriate professional degrees and certificates of completion.

We would like our colleagues to speak with power and **authority**. We would like their findings and recommendations to carry weight with their principals, to be accepted by default and to stand up to scrutiny.

We would like our colleagues to be **effective**. We would like their recommendations to result in a lower cost of security and smaller losses. We would like their recommendations to be balanced and proportional so that the sum of the cost of losses and the cost of security is minimized across time and all categories of risk.

We would like for our profession and our colleagues to be **ethical** and be perceived to be so. We would like them to be conservative and discreet. We want them to enjoy reputations for telling the balanced truth to their clients, for not raising unnecessary alarm or giving unwarranted comfort. We would like them to police themselves and each other in such a way as to maintain public trust and confidence without the need for outside authority.

We would like our practice to be **disciplined**, orderly, methodical, and rigorous. We would like our results to be self-documenting and reproducible. We would like our results to be independent of the professional who performs the work, even across national borders.

We would like our colleagues to be **current**, to be masters of the present, local, and technological situation. We want them to appreciate the current threats and threat level. We want them to appreciate the current and novel attacks. We want them to appreciate the trends and needs within business and government.

We would like our profession to be **organized** at local, state or regional, national, and international levels into mutually supporting, cooperating, and reinforcing groups and associations. We would hope to see everything from local chapters to international congresses.

We would like our profession to be **responsible and accountable** for its results. We would like to model our profession on engineering rather than theology or even medicine or law. We would like our commitments to our principals to be such that we can be measured against them and our principals can appreciate the value that they receive from us.

ISBN 1-933510-96-7/$15.00

II. Advancing the Information Security Profession

How the aspirations might be met? Map requirements for achieving the aspirations onto the institutions in our professional community that seem best able to meet it.

A. Leadership

Perhaps leadership is the requirement with largest number of sources. In promulgating this paper, the authors and their associates point a direction. However, we look to the governors and managers of every institution in our space to provide leadership. We propose a leadership council of the governors and managers of the organizations in the space. Such a council would elect its own officers, might have a permanent secretariat, and meet periodically. (Currently, $(ISC)^2$ has volunteered to serve as the secretariat for such a council.)

B. Authority, Governance

If we are to achieve our aspirations, we must have and submit to it. We must have an authority that we all recognize and accept. Most, if not all of the organizations in our space assert and enforce ethical standards. Every organization that asserts ethical standards has some responsibility to encourage conformity.

Further, organizations that function and provide services in the space should coordinate to maintain standards and avoid redundancy.

C. Organization and Discipline

The profession must be organized and the professional must identify with and participate in that organization. We must know and identify with one another. We must have institutions and associations of and for the professionals. These institutions must have high visibility within the profession. Think "church, parish, and pew." The authors believe that it is desirable for all professionals to be leaders and members in a local chapter.

While ISACA has chapters, worldwide most of their leaders come from audit. Not surprisingly, their programs focus on auditors. While ISSA leadership comes from the security profession and its programs serve the security professional, its strength is in their chapters. Chapters are both sparse and weak outside the US. While InfraGard has strong chapters and programs, its leadership comes more from law enforcement and community leadership than security and, for obvious reasons, its chapters are limited to the US. We like the model, suggested to us in the Delaware Valley, where the chapters cooperate, share calendars, and share programs to create critical mass and leadership opportunities.

We are impatient with chapter formation, particularly outside the US. We believe that international chapter formation should be the number one priority of ISSA. We encourage ISACA to help them identify constituents and leadership. If ISSA were to fail to fill this vacuum, then we must find alternatives.

D. Ethical Standards and Conformance

It is necessary that we behave ethically and that we be seen to do so. Agreed upon standards of ethical behavior are helpful, perhaps even necessary. However, they are not sufficient. Information security professionals are routinely confronted with difficult and novel ethical dilemmas. It is almost impossible to write ethical guidance sufficient for resolving all of these conflicts.

However, in a mature profession there should be documentation and publication of exemplary cases. While professionals look primarily to their peers for ethical guidance, there should be structure within the profession that facilitates and promotes such guidance and support. There should be an authority that the professional can look to for guidance in extreme or novel cases. Finally, there should be a body to which injured parties can turn to seek discipline for ethical lapses.

E. Knowledge, Skills, and Abilities

Members of the profession must have the necessary knowledge, skills, and abilities to provide competent service to their principals. Not only must they have the knowledge skills and abilities peculiar to the field but they must also have those, like reading, writing, and speaking, that they share with the other professions. They must know their own history. They must appreciate the culture in which they work.

F. Education, Training, Teachers, Masters, Mentors, and Learners

To ensure the necessary knowledge, skills, and abilities, we need both post-baccalaureate professional education and the continuing professional development required for currency and proficiency in a novel and dynamic space.

We must have educational standards, courses, and recognized curricula. We must have recognized masters, teachers, and mentors. We must know whom they are and be prepared to recommend them to others. We must respect, protect, recognize, and honor our own.

We look to academia to provide baccalaureate programs and post-baccalaureate professional programs. We look to them to exploit information and communication technology to improve both the effectiveness and efficiency of their programs.

We recognize that there is not likely to be any academic accrediting body in our space for some time. However, to provide for program quality and improvement, we propose a visiting peer review program and a formal

faculty exchange program. We look to The Colloquium (CISSE) to identify and communicate these requirements.

However, no matter how good the sources of education and training available to us, they will not be a substitute for our own commitment to life-long learning. Ultimately, we must all take responsibility for our own **continuing professional development**.

G. Credentials

Information security professionals, like other professionals, require credentials. The CISSP for example is intended to be the credential for the lifetime information security professional. However, also like other professionals, they may require special credentials from a variety of sources to vouch for necessary advanced training, knowledge, skills, and abilities for special roles or procedures.

The M.D. degree and license may authorize a physician to perform surgery.

However, they do not speak to his competence to do so. He may train for years to become a Fellow of the American College of Surgeons. Even members of this college may require additional training and credentials that speak to the part of the human body they are most qualified to operate on and what procedures they are trained to perform.

Similarly, certifications such as the CISSP do not speak to the qualifications of a professional to lead criminal investigations leading to prosecutions. This and other specialties may require additional training, experience, and credentials that speak to them.

H. Methods, Tools, and Procedures

As professionals are characterized in part by their knowledge, skills, and abilities, so a profession is characterized in large part by its methods. While methods and tools are no substitute for professional judgment and are no guarantee of good results, the absence of them is unprofessional and often produces poor results. Agreed upon methods, tools, and procedures facilitate collaboration, reduce waste, and promote quality. They encapsulate both work and special knowledge in such a way as to promote re-use.

We require methods, tools, and procedures that provide some degree of uniformity, comparability, and reproducibility of results across professionals. Such methods, tools, and procedures should reduce errors in general and particularly errors of omission. While each engagement or principal will contain novelty and may require invention, a large portion of the work should fit within the accepted methods, tools, and procedures.

As we promote good security practice among our principals, so we must promote good professional practice among ourselves. We look to academia for research, encapsulation, and dissemination of methods, tools, and procedures.

I. Measurement and Metrics

Like other professions, we need to measure our results. In the absence of measurement, we cannot know whether our results are acceptable, much less demonstrate them to others.

Most professionals measure their performance. When they cannot measure directly, they do so indirectly. For example, clergy do not measure their outcomes, but they do measure attendance and contributions.

To the extent that attempts to measure results or performance are limited, professionals measure conformance to professional standards. Medical review boards and hospital pathology committees are examples of this kind of measurement.

Measurement must be as objective as possible so that it cannot be use to arbitrarily punish those with whom we disagree to resist change.

There must be measures and metrics for results,

The authors look to the Committee on The Generally Accepted Standards of Information Security Practice (GAISSP) and COBIT/ISACA to take the lead in this area. However, this work must go far beyond what either has done to date. COBIT must go beyond mere process to content. As with methods and tools, there is a role here for academia.

J. Professional Standards and Agreements

To some extent, professions are characterized and identified by their agreement with or consent to standards of practice. For example, it is agreement with standards of practice that distinguishes doctors of medicine from those of homeopathy or criminal investigators from auditors. GAISSP is an example of such a standard of security practice as are the various ethical standards.

As professionals are identified, in part, by our sharing of a common body of knowledge, so we must be identified by shared standards of practice and conduct. It should be possible for professionals to replicate one another's work. Said another way, the results should be independent of the professionals who do the work.

We look to the Committee on GAISSP practices to identify, document, disseminate, and promote commitment to such standards. We note the absence of a successful business model for this committee and its products.

ISBN 1-933510-96-7/$15.00 ©2007 CISSE

K. Research

In spaces like ours that are both novel and innovative, we must engage in and sponsor professional research. For example, we need research to map our principles and standards onto new technology and products. Indeed much of the documented common body of knowledge for the profession is the result of research conducted by members of the profession. We need research to develop and maintain our methods, tools, and procedures.

This research must go beyond the work traditionally done by academia. Specifically it must go beyond identifying vulnerabilities. It must go beyond research into fundamental technology such as trusted systems or cryptography. It must speak to application and use. By analogy to medicine, it must go beyond making people well to how physicians should be organized and practice.

We look to academia for this research. We look to The Colloquium (CISSE) to identify and communicate the requirements.

L. Other

As the profession matures, it seems likely that additional requirements will emerge. While they may resist identification in the near term, they will become obvious and urgent in the long term. This list will do for now. The proposed leadership council might be the custodian of the requirements list and serve as the organization to establish the order and priority and report progress to the profession.

III. Conclusions

The authors suggest an aggressive program to advance the professionalism of the information security practice. They also suggest that this can only be accomplished by design and intent.

The kind of professionalism to which we aspire only emerged in medicine in the twentieth century after the Flexner Report on medical education published in 1910[1]. In law and public accounting, it was even later. This suggests to the authors that time and economics are not sufficient.

The recommendations of Flexner report were implemented in large part through the reform of medical education, in part through licensing of physicians by the state. The authors strongly prefer the former. For that reason, we have chosen to present our ideas to our colleagues at The Colloquium and challenge the profession to join with us in expanding this vision.

IV. References

[1] The Opinions expressed in this document are those of the Authors and not of their employers..

[2] Flexner A. Medical Education in the United States and Canada. New York, NY: Carnegie Foundation for the Advancement of Teaching; 1910.

[3] We assert that this effort gets too great a portion of the research dollar.

[4] http://jama.ama-assn.org/cgi/content/full/291/17/2139