Taking Professional IA Certifications to a New Level: Interview with Rolf Moulton

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

Rolf Moulton, CISSP-ISSMP< http://www.linkedin.com/pub/rolf-moulton-cissp-issmp/0/170/811 > has a long and distinguished career in information assurance. He is running for office to resume his role as a Board Member for the International Information Systems Security Certification Consortium, Inc., [(ISC)^2]< https://www.isc2.org/cgi/content.cgi?category=12 > and I was so interested by his proposals that I invited him to respond to some questions. Everything that follows is Rolf's own work with minor edits.

* * *

Rolf, what prompted your interest in information assurance (IA) from the start?

People and process. Information security was a great way to work with people throughout an organization. This was obvious to me in each of my CISO positions (Unilever, BP America & Department of Investigation). I was very fortunate to be a member of I4 (The International Information Integrity Institute) during the 1980s, and later with the ISF (Information Security Forum). Participation in these groups, as well as in many conferences and discussions, led me to the conclusion that realistic guidelines, discipline and structure, as well as both sympathetic empathy and a bit of humor, were needed to move the practice of information security forward. And that we, as information security practitioners, would benefit by defining repeatable processes to establish what needed to be done, why it mattered, what risk, cost and resource trade-offs were available to define the "what if we do" and "what if we don't" areas of opportunity, and to then get the job done. There also needed to be a way to differentiate between those people who had a sufficiently reasonable understanding of how to manage the process from those who were not yet ready to do it. So, I was already a believer in the need to establish practitioner/professional certification when I was asked to participate in the (ISC)^2 startup.

When and how did you become involved in the International Information Systems Security Certification Consortium, Inc., (ISC)^2?< https://www.isc2.org/cgi/content.cgi?category=12 >

I became involved in (ISC)^2 in 1990 when (ISC)^2 invited me to participate in the Waiver of Formal Examination (Grandfathering) Committee. The importance of the start-up of (ISC)^2 and its potential ability to provide the means to deliver both a solid credential and an enforceable code of ethics for information security practitioners (professionals) was clear – and that it would take a lot of work by many people to get it going. The credential and code of ethics, together with the continuing education requirement, could serve as the basis to start turning the information security art form into a profession.

I moved to the UK to lead the Unilever Corporate Information Security Program and was away from direct (ISC)^2 involvement for a while. Then I was invited to join the (ISC)^2 Board to fill a vacancy and was elected to the Board. While serving on the Board, the PCEO (President and Chief Executive Officer – who is the paid professional manager of the (ISC)^2 support operation) retired and a temporary PCEO was needed while a new PCEO was selected. So, I resigned from the Board and took this “temporary” assignment, which lasted 18 months. After this wonderful and unique opportunity to work directly with the membership and the operations staff ended, I was elected back onto the Board. I left the Board when the Bylaws’ term limits required that I take a break in my service. I am now standing for (re)election to the (ISC)^2 Board as an “Independent ~~c~~Candidate.”

In your view, how have the certifications programs of (ISC)^2 helped professionals, the practice of information assurance, and the world?

The CISSP, as the first (ISC)^2 certification, really got the ball rolling as the benchmark credential for defining the criteria for a reasonably knowledgeable and experienced information security professional. I personally saw it as a fundamental certification. It defined what employers should look for in hiring and/or promoting an information security professional, as well as the basis for defining parts of some academic curricula. This was a very important achievement because many practitioners could not clearly define and substantiate what they knew and understood; there also needed to be a code of ethical conduct and a requirement for continuing education. This has changed with the success and maturity of the CISSP and the certification. CISSP now also addresses areas of professional competency. For many, having an (ISC)^2 certification is a requirement for getting hired or staying in a position. The above have also influenced the hiring and promotion practices for many information security/assurance professionals internationally.

Where do you see the Consortium moving forward in the coming decade?

That will depend on what the membership and the marketplace demand and what the Board hears and delivers. I believe that there are four key areas that should be addressed as (ISC)^2 moves forward.

1. **Certification:** This is the core of what (ISC)^2 offers and there are more than 83,000 active CISSPs, as well as a smaller number of (ISC)^2 certifications that include CSSLP, SSCP and CAP. There also seem to be too many different “certifications” that are currently being offered by too many providers. This is confusing the marketplace; some rationalization is needed. There will continue to be a need for current technology practitioner *competency certificates* in contrast to *professional certifications*, such as the CISSP and the other (ISC)^2 certifications.

   The CISSP (Advanced Level) (CISSPAL), which I have proposed, has the potential to be developed as the CISSP plus a demonstration of experience and/or accomplishments. Preparing the specifics for a detailed proposal of what would define “Advanced Level” will take a good bit of research and negotiation. (ISC)^2 would benefit by collaborating with groups who have been working on this approach, such as the IISP in the UK.

   The CISSPAL was intended as a thought provoking preliminary proposal. It is very apparent from various discussions and correspondence that it is a controversial proposal. There have been strong diverse opinions:
   (1) Some CISSPs have advised that a CISSPAL is long overdue and could help to establish a professional progression;
   (2) Some have argued that now is not the time to tinker with anything that might relate to their current job or getting the next job;

(3) Others don't see the need for a change and consider this to be a needless exercise rather than an effort to advance the profession;
(4) Many others have been silent and may be waiting to see what may or may not be developed and proposed by the (ISC)^2 Board.

Clearly, a very thorough needs analysis and business case will be necessary before concluding that this is the right or the wrong approach to take at this time.

There is the potential for changes that may be suggested or required by governments and governmental agencies. Certifications have been required by some companies, governments and governmental agencies as mandatory to secure or hold a specific job. It is also not clear how this may evolve with regard to licensure in the future.

I would greatly appreciate comments and suggestions from readers sent to me< mailto:rolf.moulton@boardcandidate.com > about the need for or opposition to the preliminary proposal for the CISSPAL.

2. **Education:** Education has been a cornerstone service for (ISC)^2. In my opinion,
   - Providing education services will continue although the delivery mechanism(s) should be reviewed to provide and expand the content more easily and at a lower cost;
   - Likewise, the ability to respond to changes more quickly needs to be addressed;
   - Conferences and seminars, individually and jointly with other providers, both live and virtual, have been very successful and need to continue to be developed and offered in a wider range of formats and venues.

3. **Professional development and support:** This is an important opportunity that needs to be explored more to determine what should be done as a professional support institution and what will be demanded by the Membership – by virtue of Member participation and support. The chapter program, which I helped to initiate as part of the ALIG (Affiliated Local Interest Group) program, is part of this professional development support initiative that needs attention, with a very strong emphasis on cooperation with and support of related chapter organizations. Additionally, we worked with the ISF to get a better understanding of how to help "the next generation" of InfoSec professionals and then created the "career path" approach; this also needs more development and attention.

4. **Community Outreach:** The (ISC)^2 Foundation is a fairly new initiative. It will play a key role going forward as a means to provide service and support to the public, industry and the future for information use and protection. This will continue to be an area of continued growth that can look to providing education and policy level support on critical issues related to information and infrastructure protection.

With Rolf's permission, here's the letter he sent out to several hundred (ISC)^2 members during August, 2012.

Subject: With more than 83,000 CISSPs, when do we get an "Advanced Level" CISSP?

There are now more than 83,000 active CISSP certificate holders. The wide variations in the certificate holders' experience levels are not reflected in the current "fundamental" CISSP certification or the confusing concentrations: CISSP-ISSAP, CISSP-ISSEP and CISSP-ISSMP. This puts Advanced Level CISSPs at a recognition and a negotiating disadvantage. It also does not provide the right professional growth incentive for less experienced CISSPs.

I am taking the liberty of sending my recommended CISSP upgrade actions for the (ISC)^2 Board to you because I believe that you are concerned about protecting the value of your CISSP certification. And, because I need your help for me to bring a business case for creating the Advanced Level CISSP to the Board as an "Independent" Board Member….

To create the CISSPAL, the "Advanced Level" CISSP, I believe that the (ISC)^2 Board needs to:

- Clarify what each of (ISC)²'s certifications represents today,

- Perform a rigorous Membership and marketplace review and evaluation of all (ISC)^2 and other InfoSec certifications that are currently planned or available – including those for cloud, mobile, CND….,

- Upgrade/Create those (ISC)^2 certification(s) and related professional support that are needed,

- Implement the right marketing and support program to communicate the benefits of the CISSPAL to all CISSPs, as well as to the business and technical managers who hire and promote CISSPs.

I ask that you please sign the Petition to add my name as an "Independent Candidate" to the (ISC)^2 Board Election Ballot now by replying to this e-mail and including your (ISC)^2 Member (Certificate) Number. Or complete the Petition Form on the Board Candidate Website.< http://www.boardcandidate.com >

Then, if I am elected to the Board later this year, I can work as part of the Board to start making the priority changes that are needed to create the CISSPAL certification, as well as consider the possibly of Advanced Levels for all of the other (ISC)^2 certifications.

Thank you in advance for your consideration, help, and support – and I hope for signing my petition.

Regards,

Rolf Moulton, CISSP-ISSMP
(ISC)^2 Board of Directors Candidate
E-mail: mailto:rolf.moulton@boardcandidate.com
Website: http://www.boardcandidate.com

[Disclaimer: The opinions presented in this interview are those of Rolf Moulton, who is not currently an (ISC)^2 Board member, and they do not represent those of (ISC)^2 or the Board of (ISC)^2.]

* * *

Rolf Moulton< mailto:rolf.moulton@boardcandidate.com > has served as President and CEO (Interim) of (ISC)^2and as an (ISC)^2 Board member. Currently, he is a Director at Risk Reduction Solutions. Previously, he served as Head of IT Risk Management and Information Security at Unilever, IT Security Manager at BP America and as Director of the Computer Security Services Unit at the Department of Investigation (NYC). He holds the CISSP-ISSMP certification and MBA and BA degrees and is an active member of Information Systems Security Association (ISSA)< http://www.issa.org/ >. He helped to initiate the (ISC)^2 Chapter program, was a founding ISSA Chapter President, and was an active participant in the development of the Institute of Information Security Professionals (IISP) in the UK. He has authored many professional articles, a security management textbook< http://www.amazon.com/Computer-Security-Handbook-Strategies-Techniques/dp/0131658042/ >, and was a participating developer of BS7799 and ISO17779.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *