MARCH 19, 2018

Legaltech© news

ONLINE

An ALM Publication

Changing Cyber Law by Creating a Common Vernacular

(ISC)2, maker of the CISSP®, has launched a lexicon intended for Congressmen as well as common consumers.

BY JARED COSEGLIA, TRU STAFFING PARTNERS

With dozens, if not hundreds, of various cybersecurity certifications available for consumption in the security training and education market, one program stands alone as the oft-regarded gold standard of skill validation: the CISSP. The CISSP, which stands for Certified Information Systems Security Professional, is the flagship offering from the International Information System Security Certification Consortium. It is the most globally recognized standard of achievement in security certification aimed at giving an individual the ability to confidently design, engineer, implement and run an information security program. (ISC)2 boasts over 132,000 members in over 170 countries.

The CISSP is one of many certifications in the (ISC)2 portfolio. Security professionals can also pursue an SSCP® (Systems Security Certified Practitioner), CCSP® (Certified Cloud Security Professional), CAP® (Certified Authorization Professional), CSSLP® (Certified Secure Software Lifecycle Professional) or HCISSP®, which focuses on validating the credential holders expertise in the unique security and regulatory requirements within health care organizations.

The CISSP is not a recitation of definitions or understanding specific technology functionality, instead, it challenges candidates to leverage their real-world expertise vital to passing the exam. "What we do in CISSP is not button pushing or coding, but rather covering the entire eight domains making up multidisciplinary security best practices," states John McCumber, (ISC)2's first director of cybersecurity advocacy.

JARED COSEGLIA

(ISC)2 has developed a common body of knowledge: a peer-developed compendium CBK of what a competent professional in the security field must know, including the skills, techniques and practices routinely employed. The CBK for CISSP can be purchased along with a wealth of other self-

study resources ranging from an official training guide to *CISSP for Dummies*, a study app in the Apple store and Google Play and even official CISSP flashcards.

(ISC)2 and the CISSP differ dramatically from SANS's GIAC certification portfolio and the IAPP's CIPP/CIPM privacy accreditations in that (ISC)2 does not provide the training that is specifically for test preparation for their certifications. "We don't make cybersecurity professionals. We validate their expertise through certification," says McCumber. "We are there to provide a framework, the CISSP, so security professionals can develop a career skeleton at five to ten years and then look at how they want to specialize or broaden their discipline with us or others as the industry evolves."

Instead of exclusively offering training itself, (ISC)2 has a separate certification program for official training partners, all of which are listed based on geography on the (ISC)2 website. These partners make up a diverse array of organizations ranging from Deloitte Touche Tohmatsu Ltd. to Learning Tree International and are categorized as either Direct, Official, or Approved-tiered training providers, with Direct-tiered using official courseware developed and delivered directly by (ISC)2.

Another distinction for the CISSP is the five-year "cumulative, paid, full-time work experience" required for achievement of the endorsement. For professionals who do not meet this requirement, (ISC)2 offers an associate CISSP designation for passing the CISSP exam, then allowing up to six years to gain the prerequisite work experience. "This shows you have made a certain level of investment and attainment," adds McCumber, who has seen a notable increase in associate certifications in recent years.

Jon McCumber is new to (ISC)2 but far from a stranger to the security space. McCumber is a retired Air Force officer and former cryptologic fellow at the National Security Agency. During his military career, John also served in the Defense Information Systems Agency and on the Joint Staff as information warfare officer during the Persian Gulf War. He then spent nine years at Symantec as well as time at brands such as RSA, Mandiant and Gartner. He now represents the (ISC)2 membership and the profession at large on issues critical to the community and national security. McCumber participates in briefings on Capitol Hill with both minority and majority House committees as well as playing an active role in the Congressional Cybersecurity Caucus lead by Jim Langevin

(D-RI) and co-chair Michael McCaul (R-TX).

McCumber has had the great privilege of helping both senators and representatives better understand the world of cybersecurity especially as it relates to national security. Among all of his observations regarding the inner workings of our political system in the field of security, one stands out as overwhelmingly pertinent. "Our legislators and others are not using the right language to talk about cybersecurity," professes McCumber. "In Congress people use words like risk, threat and vulnerability interchangeably, but they are not; they actually have mathematical relationships to each other instead." Agreeing on language is a key component of passing legislation, and without clear consensus on the definition of words specific to security, laws do not get passed.

This challenge of finding a common vernacular has inspired the latest and soon-to-be-launched (ISC)2 lexicon project. "We have produced an official (ISC)2 lexicon," says McCumber. "It is not be as big as the NIST 220-page glossary of security terms, but it aims to enable everyone to easily speak the same language." This lexicon addresses defining terms as simple as "threat," for example. Is a threat man-made versus organic, hostile versus unhostile, structured versus unstructured? A frequent annoyance among cybersecurity experts is the use and misuse of the word "hacker." McCumber notes he often hears politicians and corporate executives use the phrase, "We need to hire an expert hacker," not knowing exactly what that means, but knowing they need improved security safeguards.

The new diploma will be more than just an education tool, though: it's intended to be used as leverage for congressmen and women to effect change and garner buy-in and credibility from their peers in the legislature. "We want members of Congress using the lexicon audibly and visibly so their peers and constituents can see it and hear it," adds McCumber. The commitment toward use of proper cybersecurity language intends to empower lawmakers to expeditiously find common ground using a common language. "We can all talk to each other instead of past each other if we speak the same language," gleans McCumber.

McCumber is also confident that this lexicon is a valuable asset for practicing attorneys and the news media as much as lawmakers. By combining its high-level certifications like the CISSP with a lexicon for the masses, (ISC)2 also hopes to help bridge the talent gap needed in today's high-demand/low supply cybersecurity job market. "How do we empower more people with broader backgrounds to make their way into a career in security?" asks McCumber, "First, we all learn how to speak the same language."

Jared Coseglia *is the founder and CEO of TRU Staffing Partners, an Inc 5000 Fastest Growing American Company 2016 & 2017 and National Law Journal's #1 Legal Outplacement/Career Transition Coaching category, and has over 15 years of experience representing thousands of professionals in e-discovery and cybersecurity throughout the world.*