Cybersecurity should be professionalized

It's time to institute national standards and licensing requirements for cybersecurity professionals, Pell Center says

By Jaikumar Vijayan
August 5, 2014 04:15 PM ET

Computerworld - The time is ripe for industry and government stakeholders to consider professionalizing cybersecurity, according to a report from Salve Regina University's Pell Center for International Relations and Public Policy.
Demand for cybersecurity skills is increasing exponentially, but the educational, training and certification processes to prep people for careers in the field continue to be highly decentralized, ad hoc and non-standard.

"We not only have a shortage of the highly technically skilled people required to operate and support systems already deployed, but also an even more desperate shortage of people who can design secure systems, write safe computer codes" and create the tools needed to prevent, detect and mitigate attacks and system failures, the study said.

Too many organizations lack the right skills for building and managing secure infrastructures and for dealing with attacks. And those wishing to pursue careers in cybersecurity as a career, have few clearly defined roles and career paths, the authors of study noted.

"There remains a noticeable mismatch between [the] burgeoning demand for cybersecurity talents and the efforts under way to develop professionals who can build and manage secure, reliable digital infrastructures," they wrote.

The Pell study calls for the creation of a nationally recognized association to set professional standards and education and training requirements for cybersecurity similar to what the American Medical Association (AMA) does in the medical field.

It calls on government and industry stakeholders to consider establishing professional associations for each specialty within the cybersecurity field and to develop a common body of knowledge for each specialty. In order to professionalize the field, stakeholders will also need to establish certification and licensing requirements for each specialty as well as apprenticeship and residency requirements.

In many ways, the current situation in the cybersecurity field is similar to what existed in the medical field before it was professionalized, said Francesca Spidalieri, cyber leadership Fellow at Pell Center and one of the two authors of the report.

"There were a lot of self-described doctors, but no standards," she said. "We need some kind of focal point to gather around to foster minimum, basic standards and frameworks so people have a way to navigate the cybersecurity field."

Currently, it is difficult to determine the actual skills and abilities of professionals based on their education or certification credentials, she said. It is even harder to map those skills to real-world job requirements, she said.

"There's nothing that prioritizes different educational programs. There are no standards across different specialties. There is no single organization that can take ownership of this field" as the AMA and the American Bar Association do, Spidalieri said.

Establishing a central body to oversee cybersecurity will involve the participation of all stakeholders, including employers and educational, training and private certification institutes, she said.

One way to get started might be to set up a Federally Funded Research and Development Center (FFRDC) similar to the Department of Defense's Software Engineering Institute, she noted.

The Pell report is not the first to propose professionalizing cybersecurity. The Center for Strategic and International Studies (CSIS), for instance, put forward a similar set of cybersecurity recommendations for President Barack Obama during his first term.

Critics of such proposals have argued that the sheer diversity of the field -- and the fast pace at which cybersecurity is evolving -- make it very hard to professionalize. Many have argued that cybersecurity is too broad to be treated as a single profession and maintain that the field is still too young to be professionalized.

Alan Paller, director of research at the SANS Institute, one of the largest cybersecurity training organizations in the U.S., said professionalization is practical -- but only within the technical roles. "But more than half have non-technical roles, so it wouldn't work across the whole profession."

Where skills are measurable, in areas such as forensics, incident response and penetration testing, employers and the nation deserve a better way of ensuring a person doing the work has the right knowledge and skills, Paller said.

"If it is more general, as in security management, then the variability makes reliable assessment impossible. Note, there is no certification and professional bodies for corporate management -- only for more specific, technical areas," he said.

James Lewis, senior fellow and director at CSIS, called the Pell proposal a good one, but something that will take a long time to implement.

"You need to identify what people need to know, then find a way to train and certify them," Lewis said. "There is real resistance from some job holders who are largely self-taught and the existing certification entities, who fear their business would be threatened," Lewis said. "Think how long it took to get an AMA or ABA, and we're just at the beginning for cybersecurity."

Jaikumar Vijayan *covers data security and privacy issues, financial services security and e-voting for* Computerworld*. Follow Jaikumar on Twitter at* *@jaivijayan* *or subscribe to* *Jaikumar's RSS feed* *. His e-mail address is* *jvijayan@computerworld.com*.