Shortage of cybersecurity professionals poses risk to national security

June 18 2014

The nationwide shortage of cybersecurity professionals – particularly for positions within the federal government – creates risks for national and homeland security, according to a new study from the RAND Corporation.

Demand for trained cybersecurity professionals who work to protect organizations from cybercrime is high nationwide, but the shortage is particularly severe in the federal government, which does not offer salaries as high as the private sector.

"It's largely a supply-and-demand problem," said Martin Libicki, lead author of the study and senior management scientist at RAND, a nonprofit research organization. "As cyber attacks have increased and there is increased awareness of vulnerabilities, there is more demand for the professionals who can stop such attacks. But educating, recruiting, training and hiring these cybersecurity professionals takes time."

In order to gain a clearer picture of the labor market for cybersecurity professionals, Libicki and coauthors David Senty and Julia Pollak reviewed previous studies on the topic, examined the economics of particular kinds of skilled labor shortages, conducted interviews with managers and educators of cybersecurity professionals, and examined the kinds of skill sets required for these jobs.

Libicki said the demand for cybersecurity professionals began to overtake supply in 2007, largely due to increased reports of large-scale

hacking, including the leakage of credit card data, attacks on Internet connectivity, and the discovery of "advanced persistence threats" – teams of hackers who go after intellectual property by establishing a persistent presence in the networks of U.S. and other technology targets.

The cybersecurity manpower shortage is primarily at the high end of the capability scale, commanding salaries of more than $200,000 to $250,000, Libicki said. However, many large organizations have found ways of dealing with the shortage through internal promotion and education efforts.

Some of the recommendations from the RAND study include waiving civil service rules that impede the hiring of talented cybersecurity professionals, maintaining government hiring of these professionals through sequestrations, funding software licenses and related equipment for educational programs, refining tests to identify candidates likely to succeed in these careers, and developing methods to attract women into the field.

A longer-term approach entails reducing the demand for cybersecurity professionals in the first place by limiting the use of problematic computer applications or encouraging the development of harder-to-hack operating systems.

In the meantime, Libicki also says government officials should trust that market forces and existing programs will, in time, mitigate the shortage of cybersecurity professionals. In any case, he notes that drastic steps taken today will still take years to produce results.

More information: The study is titled "Hackers Wanted: An Examination of the Cybersecurity Labor Market". It can be found at www.rand.org

Provided by RAND Corporation