NIST Publishes Cybersecurity Workforce Framework

securityweek.com

NIST Publishes Cybersecurity Workforce Framework

Tags: NEWS & INDUSTRY Training & Certification

6-7 minutes

NIST Proposes Ways for Organizations to Improve How to Identify, Recruit, Develop, and Retain Cybersecurity Talent

The National Institute of Standards and Technology (NIST) has published a cybersecurity workforce framework (PDF) to support organizations' ability to develop and maintain an effective cybersecurity workforce. The framework defines roles; necessary knowledge, skills and abilities (KSAs) for those roles; and a common lexicon to clarify communication between cybersecurity educators, trainers/certifiers, employers, and employees. It is intended to help employers develop their existing workforce, and academic institutions prepare the future workforce in a consistent manner.

Like all frameworks, it will benefit some organizations who use it, and be ignored by others. One security leader who can see potential benefits is Martin Zinaich, information security officer with the City of Tampa. In 2015, he compared the current state of cybersecurity to the slow descent and ultimate crash of Eastern Air Lines Flight 401 in 1972 -- the crew simply had insufficient awareness of what was serious and what was not so serious.

In his paper, he wrote, "National Research Council in its report, 'Professionalizing the Nation's Cybersecurity Workforce Criteria for Decision-making' (2013) stated that cybersecurity is still too new a field in which to introduce professionalization standards for its practitioners."

"Yet here we are a mere 4 years later," he told *SecurityWeek*, "and NIST is actually proposing educational workforce standards. We're slowly getting there," he added.

The NIST framework defines seven primary security workforce categories: Securely Provision; Operate and Maintain; Oversee and Govern; Protect and Defend; Analyze; Collect and Operate; and Investigate. For some, this compartmentalism is a strength; for others, it is a potential concern.

Steve Durbin, managing director of the Information Security Forum (ISF), comments, "Although the size of the information security workforce in an organization is expected to increase by more than a quarter in the next two years (according to recent ISF research), in some organizations additional staff will not be affordable. The Framework," he believes, "may further help business leaders produce retraining and ambassadorial opportunities for existing staff, in information security and beyond which will go some way to plugging what is an ever-growing skills gap in an affordable manner."

Nathan Wenzler, chief security strategist at AsTech, is not so confident. He believes it might work in a "heavily structured and siloed environment, such as the Federal government. But," he told *SecurityWeek*, "for the vast majority of organizations which are already struggling to find qualified cyber security professionals, it may work against them as more and more people are brought up through this Framework and are only adept at a single specialty. Most organizations need much more flexibility from their security personnel."

Steven Lentz, CSO and director of information security at Samsung research America, has similar concerns. "The Cybersecurity Workforce Framework is a good idea, but in reality, will companies use or pay attention to it -- that is the real question," he said.

Lentz believes that its effectiveness will depend on its reception by the existing security training companies. "How will the current security training certification sites be affected -- such as ISC2, ISACA, SANs and others? Will they participate and help develop and guide the NIST initiative, or look at it as an alternative that may not go far enough -- or as a government alternative? We all need to keep up with training," he added, "but the training partners need to work together in order for us practitioners to become stronger."

There are other practitioners with even greater concerns. One is Chris Roberts, chief security architect at Acalvio. "I'm not a fan of certificates, of degrees and of any of the formal training," he told *SecurityWeek*. "I came out of a different era, not quite the novice/apprenticeship time, but not far after it. I learned on the job and was fortunate to have some amazing mentors and a thirst for knowledge. That path does not work for everyone. We need to accommodate that in a better manner than I see here. I do not subscribe to 'you can only be a professional if you have a degree'. That's bullshit logic that is broken by so many people in the world that it needs to be banned. I do subscribe to the fact we are all individuals and this industry has been good at accommodating that and understanding that many in this field don't subscribe to mainstream education."

He may be fighting a losing battle. As any system matures, control becomes centralized. Individual bank managers can no longer decide on loans -- the decision is controlled by the central office algorithm. Chain store managers can rarely choose what they stock -- again it is controlled centrally. Political control invariably moves to the center. The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework may be another example of that centralization, currently in the form of guidance and assistance, but ultimately in the form of insistence. It will work for some, but not for others.

Steve Durbin has few doubts. "Some might say the Framework is too simplistic or too little too late but faced with the levels of shortage that many are predicting, this will at least provide organizations with guidance through what can be a very daunting process to attract and retain the right level of cyber skills."

Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.

Previous Columns by Kevin Townsend: