The Role of Professional Certification in Securing Information Systems

BY DANIEL CASTRO | OCTOBER 14, 2009

webmemo

Cybersecurity is finally getting increased attention in Washington. President Obama has made clear that securing information and communication infrastructure ranks as a high priority for his administration. This spring, the administration announced the results of the cybersecurity review conducted by Melissa Hathaway which outlined new priorities to improve security. Parallel efforts in Congress have pushed for national action to improve cybersecurity efforts, most notably the "Cybersecurity Act of 2009", legislation co-sponsored by Senators John Rockefeller (D-WV) and Olympia Snowe (R-ME).

While the Cybersecurity Act includes a number of promising reforms, one problematic idea that appears to have gained some traction is the development of a national certification program for cybersecurity professionals. While ostensibly targeted at the public sector and to protect critical infrastructure, it will have broad implications for the private sector. Such a proposal, while sounding helpful, will offer few benefits, introduce burdensome costs to the government and the private sector, and not address the root cause of most cybersecurity vulnerabilities.

The idea of a national certification for cybersecurity professionals has its roots in aa well-intentioned proposal to provide additional training and workforce development for cybersecurity in the fed-eral government, a proposal suggested by groups such as the CSIS Commission on Cybersecurity for the 44th Presidency and echoed in the 60-day cybersecurity review conducted by the Obama administration.[1] To address the shortage of skilled cybersecurity workers in the public sector, various proposals would address both demand and supply-side challenges, such as establishing a career path for cybersecurity professionals in federal government and expanding programs such as the NSF Scholarship for Service which provides funding to undergraduate and graduate students studying information security in exchange for a certain period of government service after graduation.

However, while many of these types of proposals are useful for improving the cybersecurity workforce of federal government, professional certification is not an effective policy tool to achieve this end for the simple reason that certification by itself does little or nothing to improve the knowledge, skills and abilities of workers. Instead, these certifications simply provide a means for workers and job applicants to give evidence of their competence in the field.

Professional certifications for cybersecurity such as the Certified Information Systems Security Professional (CISSP) already exist—if certifications such as these were a solution to the information security problem, we would have solved

the cybersecurity challenge many years ago. Certainly more workforce training, while not a panacea, can help teach workers how to respond to known cybersecurity attacks. But workforce training is not certification, and organizations, not Congress, are in the best position to determine what the most appropriate and effective training is for their workers. Organizations know that simply getting their employees a certification will not solve their security challenges. Having certified employees does not mean firewalls will be configured securely, computers will have up-to-date patches, or employees won't write passwords on the back of keyboards. Nor has the increase in the number of certified cybersecurity workers nationwide resulted in a decrease in vulnerabilities, security incidents or losses from cybercrime. Between 2001 and 2005, the number of CISSPs in North America grew from approximately 6,000 to 23,000.[2] But during this same period the number of vulnerabilities catalogued by the CERT Program more than doubled, the dollar loss of claims reported to the Internet Crime Complaint Center (IC3) increased more than ten-fold, and the number of complaints referred to law enforcement by IC3 increased more than twenty-fold.[3] Achieving high levels of information security require that all individuals within an organization adhere to good security practices—it is not solely in the domain of a specialized few. This is why many organizations (and most government agencies) have implemented security awareness training to create a baseline of knowledge and expectations for all workers to reduce behaviors that introduce additional risk to their information systems and networks.

This is not to say that cybersecurity professionals do not need specialized training. They do. But certification is not training. Regardless of the profession, creating a certification standard, by itself, does nothing to raise the performance of workers. As one health care scholar notes, "credentials cannot guarantee acceptable levels of productivity, nor can they guarantee quality results. Credentials simply indicate what a person should be able to do; in no way do they indicate what the person can or will do."[4] The purpose of certification is to allow others (specifically employers) to identify those workers who meet a certain standard. While a good certification standard may be a measure of a baseline level of competence, it is not an indicator of job performance. Certification (or more broadly standardized testing) can be a useful metric for measuring the size of a particular workforce or evaluating the efficacy of a training program; however, these goals can

already be achieved for the federal workforce through other means. For example, while a certification program would provide a clear metric for measuring the size and skill-level of the federal cybersecurity workforce, this data could already be obtained by surveying the number of federal workers holding information security positions. A certification program would also provide evidence of the efficacy of workforce training programs, but again, other data, such as graduation rates from new or existing training programs could similarly measure progress.

A mandate for a national cybersecurity certification for federal employees would be little more than a box-checking activity for agencies, akin to many of the Federal Information Security Management Act (FISMA) requirements that tax the federal budget and workforce, but produce few results. Consider the potential costs of such a program. For example, the U.S. Office of Personnel Management (OPM) reports over 70,000 federal workers in the GS-2210 information technology management occupational series.[5] Using the current rate charged for the CISSP certification, one of the most common certification standards for cybersecurity workers, certifying all of these workers would cost close to $40 million (not including any related test preparation costs and assuming all workers passed on the first attempt). In addition, professional certification programs, including the International Information Systems Security Certification Consortium, Inc., or (ISC)², which provides the CISSP certification, typically charge annual maintenance fees. Maintaining the certification for all of these federal workers would cost an additional $6 million per year (not including required continuing professional education credits). Private contractors, which number as many as three times the size of the federal civil service, will also have to be certified and recertified and represent another cost.[6]

In addition to the federal government, the impact of this requirement on the private sector is likely to be substantial. The proposed certification program would be national in scope and would be coordinated by the Secretary of Commerce. The latest draft of the legislation includes language that decrees, "Beginning 3 years after the date of enactment of this Act, it shall be unlawful for an individual who is not certified under the program to represent himself or herself as a cybersecurity professional." This provision means that many private sector workers would likely have to obtain this certification to continue their current job. In addition,

the bill states that "the head of a Federal agency may not use, or permit the use of, cybersecurity services for that agency that are not managed by a cybersecurity professional who is certified under the program." Broadly interpreted, this second clause could mean any online service such as Gmail or Facebook which advertises security features, such as a secure user login, would be required to be operated by IT workers with the national cybersecurity certification or else its use may not be permitted on government networks. Finally, the legislation states, "It is unlawful for the operator of an information system or network designated by the President, or the President's designee, as a critical infrastructure information system or network, to use, or permit the use of, cybersecurity services for that system or network that are not managed by a cybersecurity professional who is certified under the program." Such a requirement would likely impose certification requirements on a broad range of private network operators and companies from a diverse set of industries including telecommunications, public health, utilities and financial services. Companies will face a large expense to certify (or recertify) their workforce (although such a requirement will be a boon to certification and testing organizations), and companies will pass these costs on to consumers and taxpayers.

By requiring the certification for so many jobs, in effect, the legislation is creating a "license to practice" for cybersecurity professionals. Licenses are typically only required in professions when the public is being harmed by the absence of licensure.[7] Thus the implicit assumption in arguing for a certification program for all federal cybersecurity professionals, those involved in operating critical infrastructure, and potentially many more individuals in the private sector, is that the public is being harmed because unqualified workers are filling these jobs, not because of a lack of talent or insufficient training, but because hiring managers cannot distinguish between competent and incompetent cybersecurity workers. This is the only problem that certification (in the form of a de facto license) can fix. Yet no proponent of this provision in the legislation has provided evidence to show that this problem exists, nor is this problem commonly cited in other studies as a factor contributing to cybersecurity risks.

Another problem with a national certification program for cybersecurity professionals that is effectively a licensing standard is that it would make it more difficult to recruit qualified cybersecurity workers to government. As mentioned previously, the difficulty of recruiting skilled cybersecurity professionals to the federal workforce has been identified as a challenge, yet this proposal would effectively shrink the available workforce because, by definition, a license is restrictive in that it denies individuals not holding the license the ability to practice their chosen occupation. Already the potential workforce has been reduced because of requirements for security clearances for much of the cybersecurity work in government and critical infrastructure that eliminates many non-citizens.

But most importantly, professional certification will fail to achieve a substantial improvement in the security of all federal and critical cyber infrastructure because it does not address the root causes of vulnerabilities. A variety of causes explain existing cybersecurity vulnerabilities, perhaps the most important being that it is still difficult (if not impossible) to prove that a system is secure. For any given system, a buyer does not know how secure (or insecure) the system is because we have been unable to develop standardized measurements of risk. Since risk cannot be quantified, consumers cannot reward businesses that produce secure systems. This market failure means that financial incentives cannot be used effectively to spur stronger security. Instead, developers are generally rewarded for the features included in a system that users do see—it does not pay to develop secure systems that are often not able to be assessed by users. This is not to mean that developers ignore security risks because they will not be rewarded for it—to be sure, companies have a stake in their reputations for developing secure systems. But no major company has a flawless record on information security, and this is not a reflection of unqualified employees.

Information security is about balancing risks and rewards, and while the proposal to create a national certification for cybersecurity workers has some superficial appeal, the benefits of the proposal do not outweigh its potential costs. The measure's supporters have failed to explain how professional certification is a cost-effective measure to improve the security of our cyber-infrastructure. While professional certification may offer a "feel good" way for government to take action to improve cybersecurity, policymakers should carefully weigh the proposed benefits with the costs of such a proposal.

ENDNOTES

1. J. A Lewis, "Securing cyberspace for the 44th presidency," A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, Washington DC (2008): 15.

2. ISC2, "International Information Systems Security Certification Consortium, Inc. Annual Meeting Minutes, Miami, Florida, USA," October 15, 2005, 5, http://www.isc2.org/uploadedFiles/%28ISC%292_Public_Content/About_ISC2/Corporate_Governance/2005AMM.pdf.

3. The CERT Program is the central organization for tracking cybersecurity threats in the United States. IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NWC3). See CERT, "CERT Statistics (Historical)," February 12, 2009, http://www.cert.org/stats/ and Internet Crime Complaint Center, 2008 Internet Crime Report, 2009, 4, http://www.nw3c.org/downloads/2008_IC3_Annual%20Report_3_27_09_small.pdf.

4. Charles R. McConnell, Managing the health care professional (Jones & Bartlett Publishers, 2004), 30.

5. U.S. Office of Personnel Management, "Employment - March 2009 - FedScope," March 2009, http://www.fedscope.opm.gov/.

6. Paul C. Light, Fact Sheet on the New True Size of Government - Brookings Institution (Washington: The Brookings Institution, May 9, 2003), http://www.brookings.edu/~/media/Files/rc/articles/2003/0905politics_light/light20030905.pdf.

7. Benjamin Shimberg, "Testing for Licensure and Certification," American Psychologist 36, no. 10 (October 0, 1981): 1138.