The Cybersecurity Workforce: States' Needs and Opportunities

Executive Summary

Governors face many challenges in protecting states from the growing number and sophistication of attacks against communications networks and systems; databases containing sensitive and private information; financial, payment, and tax systems; and other critical cyber infrastructure. (The term "cyber" refers to interconnected computer systems, telecommunication networks, and wireless and wired connections to the Internet.) Cyber threats arise from a large and increasing number of adversaries seeking to penetrate those and other systems for economic gain or political or social effect. The core of a state's ability to manage, prevent, and mitigate damage from those attacks is a well-trained, stable cybersecurity workforce whose job it is to ensure the integrity and ongoing operation of the systems upon which government services have come to rely.

The most direct challenge to governors is to make sure that their states' systems are cyber secure. To that end, a first-order problem is assessing the risk of attacks and the damage they might do against what it might cost to reduce the risk of an attack or the damage done by an attack. However uncertain that assessment might be, it is among the more important elements necessary to devise a state's cybersecurity strategy, a consequence of which is what cyber skills the state needs to buy and how much it is willing to pay for them. Hiring new employees, training or retraining current employees, and contracting out for cybersecurity services are three ways that states can meet their needs. In certain circumstances the National Guard also can be used to increase the capacity of a state's cybersecurity workforce. States are well advised to have a core of employees with cybersecurity expertise who are capable of assessing the state's specific needs and making decisions about what aspects and how much of a state's cybersecurity will be provided by state employees and what aspects of it are more cost effective to contract out.

Under any strategy, a state will need a cyber workforce with a wide array of skills, from proficiency in higher-order information science to risk assessment to behavioral sciences and a variety of less demanding skills, such as those necessary to reinforce the practice of cyber hygiene day in and day out. The state will have to compete with other governmental employers and private-sector employers in the market for cybersecurity workers. That market is diffuse and complex and best thought of as an amalgamation of many smaller labor markets for skilled workers. In each of those markets, the willingness of public- and private-sector employers to pay, and of workers to respond to such inducement, will be among the key determinants of the level of cybersecurity afforded to a state or a business.

In the short term, employers will continue to draw from the pool of workers who have the skills and certifications for cybersecurity-related jobs. The availability of workers in each submarket can be different. Key market indicators include measures of vacancies against qualified applicants and, most important, trends in wages. Currently, at least in some markets for cyber workers, those indicators are sending contradictory signals. Overall demand for cybersecurity workers has risen while supply is short-term constrained; employers cite unfilled vacancies, indicating shortage. Yet for some skill sets, especially below the upper tier, wages are at best flat, indicating a market closer to a balance between the demand for and supply of cyber workers. In the longer term, the

supply of qualified workers is likely to respond to the pull of market demand, particularly if education and training programs are well aligned with that demand.[1]

The potential growth of demand for cybersecurity workers in the overall economy suggests that aligning workforce programs with that demand by training or retraining workers could be an effective approach to increasing their employability. But the challenge of protecting the state's cybersecurity assets should not be conflated with that opportunity. Rather, it should only be considered as one element of a larger and more comprehensive state strategy to improve cybersecurity. Increasing the supply of cybersecurity workers to meet a state's need to defend its cyber assets is an indirect, and likely expensive, way to achieve that objective.

In evaluating whether to steer workforce programs toward training more cybersecurity workers for the long term, governors should consider a number of factors. First, they need to evaluate the perception that demand will increase in the future against conflicting views of the adequacy of the supply of workers. Second, they should consider the issue of which skills and certifications may be necessary to meet the demand for cybersecurity workers. Most fields of work tend to sort workers into categories based on the attributes and skills necessary to do a job, and educational institutions and workforce programs respond by offering appropriate training and certifications. However, some experts warn it is premature to impose that approach on a nascent field such as cybersecurity and that an emphasis on job categorization and skill certification at this stage would be counterproductive. Third, governors should consider how fundamental cybersecurity needs might change as technology, the threat environment, and other conditions change. That could include changes in the requisite skill levels and educational background of the cybersecurity workforce.

For the Near Term, Develop a Strategy to Defend the State's Cybersecurity Assets

A first-order problem for governors is to assess the threat their state faces, develop a strategy to combat that threat, and determine how much expertise to buy. The demand for labor services is derived from the demand for the goods or services produced by the labor. The demand for labor is determined by the interplay among the market value of the goods or services the labor produces, the amount and quality of labor available, and prevailing wages. A problem common to all goods or services provided by government is that they typically are not traded in markets. National income accounts solve that problem by valuing the output of government at the cost of producing it. In the case at hand, however, the amount of cybersecurity a state should purchase is the amount that is cost-beneficial—a calculation that requires an analysis of the cost of cyber breaches, weighted by the probability that they will occur when compared with the cost of risk-reduction strategies.

A variety of individuals and groups target individual states and the federal government, including government-sponsored actors, cyber criminals, and cyb+er activists. Government-sponsored actors are interested in exploiting vulnerabilities in critical infrastructure and accessing intellectual property or trade secrets that will afford them a competitive advantage. Cyber criminals tend to target personal identifiable information or anything from which they can make a profit. Cyber activists take down or deface websites with the goal of embarrassing the targeted entity. All employ a range of tactics to achieve their goals, including advanced persistent threat campaigns, denial-of-service attacks, and phishing scams. Cyber incidents entail unauthorized access and take advantage of a vulnerability (a design flaw or a system configuration error, possibly due to the design or the system being outdated) to penetrate a system.[2] Depending on their intent, the actors may

[1] Martin C. Libicki, David Senty, and Julia Pollak, "Hackers Wanted: An Examination of the Cybersecurity Labor Market," RAND Corporation (2014) 71-74.

[2] National Research Council, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* (Washington, DC: The National Academies Press, 2014).

also introduce malware (malicious software) into the system to help achieve their goals. Since malicious actors use a variety of tactics, which constantly evolve to avoid detection, skilled cybersecurity professionals are necessary to prevent, detect, and mitigate the consequences of cyber exploitation or attack.

Regardless of the perpetrator's intent, cyber breaches are expensive for the victim. For example, one state experienced a massive breach of its department of revenue that exposed the personally identifiable information of nearly 4 million citizens. Apart from intangible costs such as loss to reputation and credibility, that breach is estimated to cost approximately $20 million to cover the breach investigation; the cost to mail notifications of the breach to taxpayers; the cost to encrypt passwords at the department of revenue; and the contract to provide credit monitoring for a year to individuals who had their personally identifiable information exposed.[3]

State governments can buy the expertise necessary to provide cybersecurity in three ways: They can train up, hire in, or contract out. Hiring a cybersecurity professional at some wage rate is essentially a statement that the professional will deliver value to taxpayers commensurate with that wage. The same is true of training up and contracting out. Practically, some minimum of in-house expertise is necessary to make a number of high-level assessments and decisions (for example, to answer the "how much to buy" question), but after that the issue is cost-effectiveness. For higher-order tasks, contracting out can offer advantages. A state might want flexibility to buy only relatively small amounts of expert services as needed. Contractors typically bring more specialized, up-to-date, and varied expertise than full-time staff. According to a recent Deloitte-National Association of State Chief Information Officers (NASCIO) survey, outsourcing can be an attractive option to chief information secutiry officiers (CISOs) who are restricted in their ability to hire workers or who have difficulty attracting employees with the needed skills sets.[4] Alternatively, a state might want the certainty of knowing that a dedicated staff of professionals is available and responsive to its needs on a full-time, continuous basis. In-house staff can be trained to know the state's specific circumstances and the culture of state government. Costs may be higher or lower than contracting out, depending on the circumstances.

After analysis, a state should have a strong understanding of the threats to digital services, operations, and stored data that drive its need for cybersecurity workers. It should know its tolerance for risk, its strategy to counter cyber threats that cannot be tolerated and mitigate the effects of intrusions, and the skills and costs needed to carry out that strategy.

Develop a strategic understanding of the state's cybersecurity risk profile, including current threats and the existing workforce capacity

States wanting to enhance their cybersecurity posture will need foundational knowledge in several key areas. States should have a strong understanding of both the threat landscape and what they are trying to protect: for example, administrative data, email communications, and electronic and Internet-based services. And they should understand the benefits and costs of various strategies to deter cyber intrusions.

Although many classified documents detail the risks states face, two open resources are available for states to use to develop a high-level understanding of their risk. The first is the NGA publication *Act and Adjust: A Call to Action for Governors for Cybersecurity*, which provides governors with high-level policy recommendations to follow to improve cybersecurity. The five recommendations touch upon governance, risk assessments, threat mitigation, compliance with

[3] Eric Chabrow, "$20 Million Loan to Cover Breach Costs," Bank InfoSecurity, www.bankinfosecurity.com /20-million-loan-to-cover-breach-costs-a-5355 (accessed June 27, 2014).
[4] Deloitte-NASCIO, "State governments at risk: Time to move forward," 2014 Deloitte-NASCIO Cybersecurity Study (2014), 20.

widely accepted security methodologies, and a risk-aware culture.[5] That document provides a first step for governors to improve state cybersecurity practices and contribute to an enterprise-wide strategy that takes the cybersecurity workforce into account.

The second resource is the National Institute for Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity.*[6] That document is more operational in nature than the previously mentioned *Act and Adjust*, providing states with a tool to assess current cybersecurity readiness and maturity in five functional areas: identify, protect, detect, respond, and recover. Taken together, the processes can help states improve their cybersecurity posture and response capabilities.[7] The framework can help states develop risk profiles that illustrate their level of cybersecurity maturity and then progress to a higher level of security.

Both resources can be useful to states in identifying their cybersecurity workforce requirements by helping them better understand their needs.

Decide Whether to Train, Hire, or Contract Out

Knowing what they want to accomplish will put state leaders in a better position to make critical decisions about how much to rely on the state's workforce to carry out its cybersecurity strategy and how much to contract out. A key advantage of contracting out, or outsourcing, is that a private-sector company that specializes in cybersecurity is much more likely to be at the cutting edge of knowledge and practice with regard to threats and the ability to detect and respond to events quickly and appropriately.[8] Contracting also allows the state to buy as much cyber protection as it needs, rather than bearing the full overhead and dedicated personnel costs associated with self-provision of cybersecurity services. Such costs can be burdensome to smaller state agencies unable to achieve economies of scale.

Many states outsource a number of key cybersecurity capabilities by buying managed security services (MSS) from private-sector companies. By using MSS, a state can more rapidly and effectively detect, defend against, and mitigate cyber attacks and vulnerabilities. To help states bolster those capabilities, the U.S. Department of Homeland Security (DHS) has made available to all federal departments and state and local governments continuous diagnostics and mitigation (CDM) services at reduced costs.[9] Under the CDM program, DHS has partnered with the General Services Administration to give all federal departments and agencies, state, local, regional, and tribal governments access to a multiple-award blanket purchase agreement that offers monitoring-related products and services.[10]

States also are outsourcing other key functions, including cybersecurity awareness and training programs. For example, **Maryland** and **Michigan** recently outsourced workforce cybersecurity awareness training programs by contracting with an outside vendor. Both states have reported improvements in cybersecurity awareness in their workforces.

But outsourcing has its disadvantages and risks. For one, expertise to perform a service lies outside govern-

---

[5] National Governors Association, *Act and Adjust: A Call to Action for Governors for Cybersecurity* (Washington, DC: National Governors Association, September 2013), http://www.nga.org/cms/home/nga-center-for-best-practices/center-publications/page-hsps-publications/col2-content/main-content-list/act-and-adjust-a-call-to-action.html [6] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (February 12, 2014). http://nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

[7] Ibid.

[8] Public CIO, "Cyber-Security Essentials for State and Local Government," (2011), http://www.corp.att.com/stateandlocal/docs/cyber_security_essentials.pdf.

[9] Department of Homeland Security, "A Major Step Forward in Better Protecting Federal, State and Local Cyber Networks," August 13, 2013, http://www.dhs.gov/blog/2013/08/13/major-step-forward-better-protecting-federal-state-and-local-cyber-networks, (accessed June 27, 2014).

[10] U.S. General Services Administration, "Continuous Diagnostics and Mitigation," http://www.gsa.gov/portal/content/176671?utm_source=FAS&utm_medium=print-radio&utm_term=cdm&utm_campaign=shortcuts, (accessed June 27, 2014).

ment and must be continually purchased from a private-sector provider. The state does not build internal expertise and could become too dependent on its contractors. The private contractor could go out of business, leaving the state needing to restore vital lost services or capabilities with little or no notice. Furthermore, a private contractor might not provide the same level of diligence in safeguarding sensitive data held by the state—such as personal information about citizens—as would state employees. Accordingly, some states are beginning to look for ways to NIST's cybersecurity framework in contracts with outside companies.

When considering strategies to expand state capacity, governors also should consider the role of the National Guard. Although the National Guard is not in a position to supplement a state's normal day-to-day cybersecurity operations, there are two areas in particular where the Guard can be an essential asset. First, at the governor's direction, the National Guard's cyber expertise could be used to coordinate, train, advise, and assist state agencies in performing vulnerability assessments of information networks and systems. For example, through Michigan's Cyber Range, the National Guard along with other partners can engage in penetration testing or "red teaming" to simulate an adversary's view of the system and expose cybersecurity vulnerabilities. The results of the assessment can be used to improve network defenses and inform the allocation of additional resources and mitigation measures. In addition, the National Guard can play an important role in cyber incident response. Because of its unique role serving both governors and the President, the National Guard is well-positioned to support cyber incident response and recovery operations, to include assistance to law enforcement entities under state and federal law. States such as Delaware, Maryland, Michigan, Rhode Island, Utah, and Wisconsin, as well as others, each have established units to support state responses to cyber attacks.[11]

Of course, as with all buying decisions, a state will need to carefully weigh the balance of benefits, costs, and risks of each strategy. A good place to start is to assess the capacity to provide cybersecurity needs internally.

Evaluate State Employees' Capacity to Provide Cybersecurity

In any scenario, a state will want to fill at least a portion of its cybersecurity needs by direct hire or upgrading and retraining its workers. In doing so, it will face two key challenges: first, it must have a strong understanding of its specific need for skilled workers, the available supply of such workers, and the capabilities of its existing workforce. Second, a state should understand how its employment policies affect its ability to fill needed capabilities by improving recruitment, retention, or training of its workforce. Many experts rate the policies of the average state as inadequate for those tasks.

The cybersecurity workforce is an amalgam of information technology (IT) workers (itself a catch-all category), behavioral scientists, risk analysts, and other professionals. It consists of workers in the private and nonprofit sectors, the public sector at all levels (state, local, tribal, territorial, and federal governments), and the military. The cybersecurity workforce plays a wide variety of roles and shoulders responsibilities that require a blend of knowledge, skills, and capabilities in behavioral, management, and technical fields. Because of the wide range of talents needed, there is no single market for states to draw from to meet their cybersecurity workforce needs. Most discussions and analyses of the labor market for cybersecurity workers tend to focus on IT workers and workers with STEM backgrounds. The following discussion draws on such analyses. At the same time, it bears keeping in mind that IT and cybersecurity workers are not synonymous.

---

[11] [1] Homeland Security News Wire, "National Guard Units Help States Ward Off Cyberattacks," Homeland Security News Wire, February 3, 2014, http://www.homelandsecuritynewswire.com/dr20140203-national-guard-units-help-states-ward-off-cyberattacks.

One resource to help states identify their workforce needs is the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework. It defines the cybersecurity workforce using standardized terms that differentiate among professions by function: secure provisioning; operations and maintenance; protection and defense; investigations; collections and operations; analysis; and oversight and development.[12]

States also can look to a recent National Research Council report that assesses the current landscape for cybersecurity workforce development. That report establishes criteria that organizations can use to consider which specialty areas may require professionalization.[13] The report concludes that states might not want to be bound by such a defined taxonomy of skills, which could prematurely limit the pool of potential workers. Though appearing to be in conflict, the two approaches, when taken together, provide states with valuable insights about necessary functions and ways of flexibly seeking and training workers to perform them.

The following considerations are designed to help states further understand market conditions for skilled cyber professionals and the ability to recruit and retain them.

Assess the state's cybersecurity workforce supply by surveying job postings, wage and salary data, and state employees

Workforce supply conditions can be gleaned in various ways. States can, for example, build on a methodology developed by Change the Equation (CTEq), a nonprofit initiative aimed at improving the quality of STEM learning in the United States.[14] CTEq measures the demand for workers to fill STEM skill-related jobs, which included IT and cybersecurity professions. CTEq's *Vital Signs* provides a state by state snapshot of the supply and demand of STEM skills. Comparing average monthly online job postings with average monthly unemployment figures, CTEq recently found that overall unemployed people outnumbered job postings by almost four to one, whereas the relationship was reversed for STEM occupation job postings, which outnumbered unemployed people by two to one.

The CTEq study illustrates the shortage of STEM talent and differences in demand for certain skill sets. For example, there were about 1.4 computer programming job postings for every unemployed computer programmer but more than four network and computer systems administration jobs for every unemployed administrator.[15] Conditions vary among states as well as among job categories. For example, **Delaware**'s STEM job postings outnumbered the STEM unemployed about three to one, in contrast to **Michigan**, where there was about a one-to-one ratio. Being aware of its specific circumstances can help a state identify strategies for meeting its cybersecurity workforce needs.

Wage data are another indicator of the state of the market for cybersecurity workers in the IT field and present a mixed picture. According to InformationWeek's 2013 Salary Survey, the median staff annual salary for cybersecurity professionals was $95,000 in 2013, down $2,000 from the previous year. The Economic Policy Institute analyzed data from the U.S. Census Bureau's Current Population Survey and concluded that the real wages paid to workers in the computer and information technology

---

[12] NICCS.us-cert.gov, "Interactive National Cybersecurity Workforce Framework." National Initiative for Cybersecurity Careers and Studies, http://niccs.us-cert.gov/training/tc/framework (accessed June 26, 2014).
[13] National Research Council. *Professionalizing the Nation's Cybersecurity Workforce: Criteria for Decision-Making* (Washington, DC: The National Academies Press, 2013).
[14] Changetheequation.org, "About Change the Equation." Change the Equation, http://changetheequation.org/about-change-equation (accessed July 3, 2014).
[15] Changetheequation.org, "STEM Help Wanted: Demand for Science, Technology, Engineering and Mathematics Weathers the Storm." Change the Equation, http://changetheequation.org/sites/default/files/CTEq_VitalSigns_Supply%20%282%29.pdf (accessed July 3, 2014).

occupations have been flat since the late 1990s.[16] But according the Information Week survey, management salaries for cybersecurity professionals rose $5,000, to an average of $120,000 from 2012 to 2013. Both staff and management salaries are higher than the salaries for general IT staff and management, which average $87,000 and $110,000, respectively.[17] Additionally, cybersecurity salaries for some higher-skilled positions continue to increase to match the growing demand. For example, information security analysts, systems security administrators, network security engineers, information systems security managers, and chief security officers saw a salary increase from 8 percent to 13 percent from 2011 to 2013.[18]

A survey of state chief information officers (CIOs) and chief information security officers (CISOs) found that despite training programs, significant gaps remain in the skills of state cybersecurity professionals. To highlight the disparity in skills that were needed compared with the skills possessed by employees within the state. In 2006 **New York** conducted an IT skills assessment that included two voluntary surveys. One was directed to IT employees in the general state workforce; the other was to CIOs in state agencies. The surveys produced a comprehensive report that includes self-reported demographics, skill proficiencies, and training needs of the state IT workforce, as well as agency-level IT forecasts for the next three years.[19] The data served as the basis for an action plan for the New York State CIO Council to enhance the professional development of the state IT workforce.

Additionally, more than half of survey respondents reported difficulty in recruiting new employees to fill vacant IT positions, and only 32 percent of CIOs said that their staff members have the requisite cybersecurity competency.[20] In 2011, in a survey of state CIOs forty-one states indicated that offering competitive wages is a challenge to attracting and retaining IT professionals, citing the negative effect of the civil service system.[21] Similar findings were also identified in the 2014 Deloitte-NASCIO survey where nine in ten respondants identified salary as the biggest challenge to attacting talent to state cybersecurity positions.[22]

Improve retention and quality of the workforce through human resource policies and training

In the short term, in circumstances of constrained supply and increased demand, states that want to increase or upgrade their cybersecurity workforce will most likely need to improve compensation and other employment policies such as training.

One of the most difficult challenges facing state agencies is the loss of skilled workers to the higher-paying private sector. To help stem those losses, governors can reform human resource policies to improve parity with the private sector. Some states addressed retention through salary adjustments by transitioning the IT workforce to an at-will status (a standard practice in the private sector) or reclassifying job titles.

Delaware's Department of Technology and Information developed a compensation plan that operates

---

[16] Hal Salzman, Daniel Kuehn, and B. Lindsay Lowell, *Guestworkers in the High-Skill U.S. Labor Market* (Washington, D.C. : April 2013), 17-20.
[17] Robert Lemos, "Security Job Market 'Rockin,' But Pressures Rise," *Information Week*, April 2013, http://reports.informationweek.com/abstract/166/10337/Professional-Development-and-Salary-Data/Research:-2013-Salary-Survey:-Security.html?cid=nl_iwkrnwsl0409 (accessed July 7, 2014). [18] RobertHalf.com, "Salary Guides Robert Half Technology 2011, 2012, and 2013 IT Salary Guides."
[19] Center for Technology in Government, "New York State Information Technology Workforce Skills Assessment Statewide Survey Results" Summary of Results (Center for Technology and Government, December 12, 2006) http://www.ctg.albany.edu/projects/pubs?proj=nysit&sub=pubs (accessed June 27, 2014).
[19] National Association of State Chief Information Officers, 2012 Deloitte-NASCIO Cybersecurity Study (NASCIO, 2012). http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2012.pdf (accessed June 27, 2014).
[20] National Association of State Chief Information Officers, *State IT Workforce: Under Pressure* (National Association of State Chief Information Officers, January 2011) http://www.nascio.org/publications/documents/NASCIO_ITWorkforce_UnderPressure.pdf (accessed June 27, 2014).
[21] Deloitte-NASCIO, "State governments at risk: Time to move forward," 2014 Deloitte-NASCIO Cybersecurity Study (2014), 18.
[22] State of Delaware's Information Services Task Force Report to Governor Ruth Ann Minner, E-Volution: Redefining Delaware's IT Management Strategy for the 21st Century, May 8, 2001.

outside of the civil service system.[23] By becoming a pay-for-performance organization, the flexible system lets the state adapt job titles, functions, and responsibilities quickly to meet technology needs. Additionally, the salary structure allows compensation that is approximately 20 percent to 30 percent higher than in a traditional merit-based compensation system.

Colorado aligned state pay ranges with private sector market rates, which has led to competitive base pay levels.[24] **Pennsylvania** reclassified IT jobs and increased the salaries of 80 percent of its IT workers to more competitively compensate staff.[25]

Making a state more cyber secure involves more than having a cadre of workers designated for cybersecurity. The greatest cybersecurity vulnerabilities come from people. Even in well-defended networks, poor cyber hygiene by employees, such as clicking on inappropriate links or employing weak passwords, can compromise a system. All state employees connected to the Internet or to state networks must receive ongoing training on good cybersecurity practices.

In addition to general training, states also may want to consider third-party certifications for certain positions. The National Initiative for Cybersecurity Careers and Studies is a resource states can use to weigh whether a position requires additional certifications.[26]

Creating an inventory of positions that might require certifications can be a step toward upgrading the state's workforce: states could offer continuous training to workers in designated cybersecurity positions and provide new training to workers in other positions who might have the interests and skills needed to move into a cybersecurity job. Drawing workers from elsewhere within state government would be consistent with recommendations of the National Research Council and let the state better align its workforce with its needs.

State cybersecurity training programs can be extended to contractors and other Internet users. With that aim, **Michigan** has launched an innovative security awareness training for all state employees and has posted online guides available to the public with the goal of reducing risk. The program, which won an award from NASCIO, consists of interactive and targeted lessons to change the security culture.[27] In addition to state employees, more than 60,000 end users and partners are enrolled in Michigan's online cyber awareness program. **Maryland** has adopted a similar cyber awareness program, recognizing it as a best practice training tool for state employees.

Peering into the Future

After analyzing the various considerations previously discussed, a state will be better positioned to make decisions about the extent to which it might choose to bolster its workforce or contract out for at least a portion of its cybersecurity needs. Additional consideration should be given to evaluation of the likely future paths of both cyber threats and cybersecurity. Although cyber threats do not now appear likely to diminish, such a turn of events cannot be ruled out. Better security solutions built into hardware and software could diminish demand for cybersecurity workers.

The need to make decisions in the face of an unknowable future is not unique to cybersecurity. The best that can be done is to make well-informed decisions, always allowing for flexibility to adjust to conditions as they change.

---

[23] Colorado Office of the State Auditor, Evaluation of the Department of Personnel & Administration's Annual Compensation Survey for Fiscal Year 2014, May 17, 2013. http://www.leg.state.co.us/OSA/coauditor1.nsf/All/BF34709D606F20B587257B74006681E6/$FILE/2199%20DPA%20Comp%20Survey%2005%2020%2013%20Final.pdf

[25] "Commonwealth of Pennsylvania Retention and Recruitment," 2002 NASCIO Award Nomination.

[26] NICCS.us-cert.gov, "Professional Certification" National Initiative for Cybersecurity Careers and Studies, http://niccs.us-cert.gov/training/professional-certifications (accessed June 27, 2014).

[27] Nascio.org, "2013 NASCIO Recognition Award Nomination," National Association of State Chief Information Officers, http://www.nascio.org/awards/nominations2013/2013/2013MI10NASCIO%20Security%20Award%202013%20Final.pdf (accessed July 3, 2014).

For The Long Term, Align State Education and Workforce Programs to Support Training of Cybersecurity Workers

A second problem for governors is resolving how much to invest in education and training of citizens seeking jobs in the cybersecurity workforce. The decision to deploy state resources to increase the supply of cybersecurity professionals should be made as part of a state's workforce strategy, rather than as a response to difficulties the state might have in hiring cybersecurity professionals. The demand of each state is only a portion of the overall market, and steering state resources toward increasing the supply of expertise so that it will be available to government at a lower wage is certainly more expensive than raising wages for state workers or paying for consulting services. That said, partnerships between educational institutions funded by states and businesses that focus on increasing the supply of cybersecurity professionals can provide skills that the market demands and offer graduates an advantage in securing employment—an objective of workforce, rather than cybersecurity, policy.

Some caveats exist in addressing the perception of a future shortage of cybersecurity workers. Although the future demand for cybersecurity workers appears strong today, technology could change in such a way that information systems become more secure and the demand for cybersecurity workers is less strong than anticipated, a circumstance that has played out in other professions in the past (for example, aerospace engineering, which was a growing profession through the 1980s, experienced a 35 percent drop in employment in the early 1990s).[28] Even if overall demand increases as projected, the skills of workers who provide cybersecurity services in the future can't be known with certainty. A current excess supply of workers in areas like computer programing attests to how difficult it is to predict future demand for specific skills, even within a broad category of growing demand. In today's market, the National Research Council report observes that many cybersecurity workers have not been formally trained as cybersecurity experts. Thus, future demand also could be met by workers not trained as cybersecurity experts.

A longer-term challenge is ensuring that states' education and workforce pipelines support the projected growth in cybersecurity jobs. Based on current data for the most common computer and information technology occupations related to cybersecurity, the U.S. Bureau of Labor Statistics projects an increase of almost 650,000 in the number of people employed in those occupations between 2012 and 2022.[29] That growth is faster than that projected for all occupations and does not include other non-technical cybersecurity occupations, such as attorneys, policymakers, and managers. Taken together the BLS's projections suggest that governors seeking to improve the future employment prospects of their citizens should ensure that current education and workforce programs include a focus on the computer and information technology occupations and, in particular, those related to cybersecurity.

One challenge to attracting more qualified individuals to the field might be that the millennial generation (in this case, defined as ages 18 to 26) is not being encouraged to consider careers in cybersecurity.[30] According to a recent survey of millennials, 82 percent of those surveyed noted no high school teacher or guidance counselor ever mentioned the prospect of

---

[28] U.S. Department of Labor, Bureau of Labor Statistics, "Employed persons by detailed occupation and sex, 1983-2002 annual averages." http://www.docstoc.com/docs/92288304/BLS-update-of-Employed-persons-by-detailed-occupation-and-sex-1983 (accessed October 1, 2014).

[29] BLS.gov, "Occupational Outlook Handbook: Computer and Information Technology Occupations." Bureau of Labor Statistics, http://www.bls.gov/ooh/computer-and-information-technology/home.htm (accessed September 26, 2014).

[30] Raytheon, "Preparing Millennials to Lead in Cyberspace," (Sterling, VA: Raytheon, 2013), http://www.raytheon.com/capabilities/rtnwcm/groups/gallery/documents/digitalasset/rtn_158203.pdf (accessed July 7, 2014).

a cybersecurity career.[31] Governors seeking to help educate and train citizens for good jobs could consider actions that will help attract a younger generation of qualified individuals for jobs in cybersecurity and related IT fields.

Designate computer science as a STEM course

Science, technology, engineering, and mathematics (STEM) courses are required for graduation from the K-12 education system. Computer science and other cybersecurity-related coursework do not count as STEM credits in most states. More students may be drawn to cybersecurity and other IT fields if computer science fulfilled a graduation requirement. To accomplish this, governors may need to consider adjusting state education requirements.

Several states already are moving in that direction. Currently, 14 states and the District of Columbia allow a computer science course to count as a required graduation credit for either mathematics or science. After a study revealed that 77 percent of voters agreed that computer science should count as a STEM credit, **Washington** allowed Advanced Placement computer science to fulfill the high school STEM graduation requirement.[32]

Assess the capacity of educators and schools to meet the needs of the cybersecurity workforce

Though experts focus on a shortage of interested students and skilled workers, there also is a similar shortage of teachers qualified at the K-12 level to teach foundational cybersecurity skills, in particular those related to information technology and computer science. Additionally, many schools lack necessary equipment and resources (computers, broadband, etc.). If teachers are unqualified or schools ill-equipped, K-12 students—many of whom will be the states' future prospective workers—will not be exposed to cybersecurity during their formative years, a prime time to pique their interest.

Compounding the issue is the fact that each state has its own definition of computer science and its placement in curricula, as well as who is qualified to teach it. A report by the Computer Science Teachers Association found that only **Arizona** and **Wisconsin** require K-12 teachers to be licensed in computer science to teach the subject.[33] That does not necessarily mean that K-12 teachers elsewhere are unqualified to teach such material; other factors such as experience, education, and practical skills may also need to be considered. Nevertheless, the lack of teacher certification is a worrying indicator of the value the educational system places on computer science.

The CTEq *Vital Signs* resource also can help states assess the capacity of educators and schools to teach cybersecurity skills. *Vital Signs* includes information about students' access to learning opportunities and the resources schools and teachers have to teach STEM courses. By using such information, governors can make more informed decisions to address potential areas of need.

Use the community college system

Many students and professionals seeking a career change or professional development seek help through community colleges. The National Science Foundation (NSF), through the Cyber Security Education Consortium (CSEC), assists community colleges trying to enhance their information assurance and computer forensics programs.[34] Those efforts contribute to developing a qualified cybersecurity workforce in **Arkansas**, **Colorado**, **Kansas**, **Louisiana**, **Missouri**, **Oklahoma**, **Tennessee**, and

---

[31] Ibid.

[32] Washington STEM, "Statewide Survey: Math and Science Skills Help Students and the Economy," Press Release, February 20, 2013, http://www.washingtonstem.org/News-Media/Press-Releases/Statewide-STEM-Poll-Feb-2013#.U0LqLTbD_X4.

[33] Computer Science Teacher Association, "Bugs in the System: Computer Science Teacher Certification in the U.S." (New York, NY: Association for Computing Machinery, Inc., 2013), http://csta.acm.org/ComputerScienceTeacherCertification/sub/CSTA_Bugs InTheSystem.pdf (accessed July 7, 2014).

[34] CSECOnline.net, "Cyber Security Education Consortium," Cyber Security Education Consortium, http://cseconline.net/ (accessed July 7, 2014).

Texas. Since its inception, CSEC has helped structure academic programs at more than 25 community colleges and contributed to the training of more than 600 students and several thousands of workers.

NSF also has funded the National CyberWatch Center and other regional centers, such as CyberWatch West and the National Center for Systems Security and Information Assurance (CSSIA) in an effort to advance cybersecurity education and strengthen the national cybersecurity workforce.[35] The National CyberWatch Center focuses on all levels of cybersecurity education but especially tries to highlight opportunities in the community college system. Similarly, the CSSIA National Resource Center aims to enhance cybersecurity programs at historically minority and underrepresented academic institutions to attract more prospective workers to the field.[36]

Additionally, the National Security Agency and DHS sponsor the National Centers of Academic Excellence (CAE). The CAE are recognized for having the leading programs in information assurance, cybersecurity, and research at four-year and community colleges. Expanding the number of centers could provide states with more specialized education opportunities to help students develop careers in cybersecurity.[37]

Employ partnerships with academic institutions and the private sector

States can use public-private partnerships to share expertise and resources in order to offer education and training opportunities for interested and talented students. Private-sector partnerships are generally underused and present governors with a way to increase the number and quality of cybersecurity workers in their state.

One such partnership is the CyberCorps: Scholarship for Service (SFS) program.[38] Through SFS, NSF issues scholarship grants to attract students to IT fields at select colleges at the undergraduate, graduate, and doctoral levels. Scholarship recipients are expected to serve at a state, local, tribal, or territorial (SLTT) or federal government organization in an IT-related position for a period equivalent to the length of the scholarship. The program, however, is currently underused by states. Between 2008 and 2012, there have been 793 graduates, with only 23 placed in SLTT government positions.[39] This disparity is partly due to better recruitment and compensation by the federal government. Governors can promote SFS to rectify this disparity and encourage talented students to remain in the state after graduation. However, because SFS is a federal program designed to attract federal workers, governors may want to consider establishing their own state-focused SFS-type program.

Another organization that helps states identify and foster prospective talent is Cyber Aces, a foundation dedicated to assisting young professionals develop cybersecurity practical skills.[40] Seven states currently host Cyber Aces competitions, which are open to students who excel during the free online training. Top performers in the program become eligible for elite scholarships toward specialized training, internship opportunities, and high-paying jobs.

---

[35] CyberWatchCenter.org, "National CyberWatch Center: About Us," CyberWatch Center, http://cyberwatchcenter.org/ (accessed August 25, 2014).
[36] CSSIA.org, "National Center for Systems Security and Information Assurance (CSSIA)," Center for Systems Security and Information Assurance, http://www.cssia.org/ (accessed August 25, 2014).
[37] NSA.gov, "National Centers of Academic Excellence," The National Security Agency, http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml (accessed July 7, 2014).
[38] SFS.OPM.gov, "CyberCorps: Scholarship for Service." U.S. Office of Personnel Management, https://www.sfs.opm.gov/default.aspx (accessed July 7, 2014).
[39] NSF.gov, "National Science Foundation, Directorate for Education and Human Resources." National Science Foundation, http://www.nsf.gov/dir/index.jsp?org=EHR (accessed July 7, 2014). [39] Cyberaces.org, "Cyber Aces." Cyber Aces, http://www.cyberaces.org/(accessed July 7, 2014).
[40] Cyberaces.org, "Cyber Aces." Cyber Aces, http://www.cyberaces.org/(accessed July 7, 2014).

The private sector is working with state educational institutions to develop the next-generation IT workforce. In **Louisiana**, the IBM Services Center: Baton Rouge project intends to expand higher education programs in computer science fields as well as create technology career opportunities. Louisiana State University, with funds from this project, plans to double its computer science faculty and triple the number of computer science graduates within the next five years.[41] IBM will work closely with professors to tailor coursework to match the skills needed for the future workforce.

Conclusion

By considering the recommendations outlined above, governors can make significant strides in addressing cybersecurity challenges. Those recommendations include both short-term and long-term strategies such as analyzing your state's cybersecurity needs, considering whether to hire in or contract out, evaluating workforce supply and demand, improving workforce retention through training and human resource reforms, and for the longer term aligning state education and workforce programs to train citizens for cybersecurity jobs.

Laura Saporito
Policy Analyst
Homeland Security & Public Safety Division
NGA Center for Best Practices
202-624-5413

October 2014

The author would like to thank a number of individuals whose input and comments were essential to the writing of this Issue Brief. Those individuals include David Behen, State of Michigan; Elliot Schlanger, State of Maryland; Dr. Farnam Jahanian, National Science Foundation; Dr. Diana L. Burley, George Washington University; Doug Robinson, National Association of State Chief Information Officers; David Brown, Cyber Aces Foundation; Ned McCulloch, IBM; Dr. Emily Grumbling, National Science Foundation; Dr. Keith Marzullo, National Science Foundation; Dr. Victor Piotrowski, National Science Foundation; Dr. Eugene H. Spafford, Purdue University; Dr. Sujeet Shenoi, University of Tulsa; Cheri Caddy, National Security Council; Alaina Clark, Department of Homeland Security; and Dana Thompson, Maryland Governor's Office.

Support for the NGA Resource Center for State Cybersecurity comes from: American Gas Association, Citigroup, Deloitte, Edison Electric Institute, FireEye, Hewlett-Packard, IBM, Intuit, Nuclear Energy Institute, and Symantec.

Recommended citation format: L. Saporito, *The Cybersecurity Workforce: States' Needs and Opportunities* (Washington, D.C.: National Governors Association Center for Best Practices, October 27, 2014).

[41] Office of Governor Bobby Jindal, "Governor Jindal and IBM Senior Vice President Colleen Arnold Break Ground on New 800-Job Technology Center in Downtown Baton Rouge," Press Release, September 26, 2013, http://gov.louisiana.gov/index.cfm?md=newsroom&tmp=detail&articleID=4260.