States Confront the Cyber Challenge

Building a Cybersecurity Workforce Pipeline

The Workforce Gap

States confront four interrelated challenges to building, recruiting, and retaining a cybersecurity workforce. First, many companies are unable to find or hire employees who possess the skills necessary for writing computer code, analyzing network traffic, using security applications, or managing cybersecurity projects. Second, while graduates with these skills often find employment, supply remains limited because schools struggle to attract new students to the field or find the resources to educate those who do show interest. Third, there is a gap in finding qualified teachers to educate students in this field. Finally, cybersecurity specialists frequently choose lucrative positions in the private sector, leaving resource-strapped government agencies struggling to fill even the most basic positions. These four problems combine to create a cybersecurity workforce shortage that holds back state economic development and imperils government networks.

Questions for Governors

- How does cybersecurity and, more broadly, technology fit into long-term economic development plans?
- What is the unmet demand for cybersecurity workers in my state?
- What is the landscape of computer science and cybersecurity education throughout K-12 and higher education?
- In what area does my state face the most acute shortages: open positions, cybersecurity specialists, non-cybersecurity employees with a cybersecurity background, demand for cybersecurity courses, or supply of instructors?
- How are schools and companies having a dialogue to build a pipeline from cybersecurity programs into the private sector?
- Does the state provide any incentives for students to go into these fields?
- What kind of cybersecurity employees do state agencies need?

Recommended Steps for Governors

(1) *Articulate and communicate a vision for a 21st century workforce*.

Success in workforce development requires coordination between government and private industry, and such cooperation can be difficult without shared goals. Some states enjoy inherent historical, geographical, and population advantages that attract technology companies. Other states may not be positioned to become cybersecurity hubs, but host companies who need more cybersecurity workers. Economic growth elsewhere depends on advanced manufacturing skills, as differentiated from software-specific talent. Governors should evaluate where their state fits into the national economy now, how they want that to change, and craft a vision for their state's future workforce.

(2) *Convene educators and private industry to assess the needs of students and businesses.*

Governors need to obtain situational awareness of the cybersecurity ecosystem by gathering private companies, government bodies, and schools to identify workforce gaps. Diversity of representation is key: large employers who regularly hire large numbers of cybersecurity workers might not face the same obstacles as do smaller firms, and four-year universities differ sharply from community colleges.

(3) *Treat cybersecurity as an industry-wide technology problem that demands more than additional computer science courses*.

Principles of computer science form the foundation of cybersecurity, but many companies do not need more graduates in computer science. Cybersecurity workers also include those trained in network analysis, hardware engineering, or general project management—fields that some students might prefer over computer science. Moreover, cybersecurity jobs include non-technical positions for which cybersecurity is a constant consideration. When convening educators and private industry to formulate solutions, governors should ensure to address whether and how to address these broader aspects of workforce development.

(4) *Identify, establish, and promote mid-career training programs*.

Better cybersecurity does not require hiring graduates of elite institutions with academic credentials. Some employers simply need skilled workers who understand risk assessment and can utilize security applications—skills that can be taught to IT professionals who want to advance their career, or to lesser-skilled workers who want to enter a new field.

(5) *Promote non-traditional conduits for budding cybersecurity workers*.

Policies that discourage selecting employees who lack formal academic credentials can stymie otherwise qualified candidates. Governors should work with credentialing agencies and private companies to make it easier for non-traditional institutions (such as coding boot camps and competitions) to credential participants, while encouraging companies to grant internships and apprenticeships based on demonstrated ability, regardless of academic pedigree.

(6) *Boost the supply of students by enhancing interest in computer skills and cybersecurity by introducing relevant subjects earlier in their education*.

Schools might prefer to offer more computer-related courses, but cannot find enough students to fill the classes. Some students might have little interest in technical subjects, while others who do envision a future in cybersecurity may believe that earning a doctorate in computer science is the only path. Governors should work with the requisite authorities to reach out to students and introduce relevant subjects at an earlier age. For example, logic games or age-appropriate coding competitions can be a fun way to teach the basics of computer science before secondary school.

(7) *Expand the supply of educators by drawing on adjunct talent and training current instructors.*

Some schools do enjoy increasing demand for courses involving cybersecurity and computer science. But those institutions, whether in K-12 or higher education, often struggle to find instructors to run those classes and mentor students. Governors should work with the relevant state and local bodies to address this shortage in at least two ways. First, they should consider amending licensing rules to attract adjunct instructors who possess the proper skills, but lack formal qualifications needed to teach in public schools. Second, states should encourage private industry to train credentialed instructors in K-12 who already have an interest in teaching cybersecurity subjects, but who lack specific skills that they can teach.

Please e-mail Timothy Blute, Program Director, Homeland Security and Public Safety Division, NGA at: tblute@nga.org *with any questions.*