NATIONAL CONFERENCE *of* STATE LEGISLATURES

The Forum for America's Ideas

NCSL Executive Committee on Cybersecurity

Cyber Education and Training

Cyber education encompasses two fronts for state government—educating state employees on the correct and safe use of state systems, and cultivating and promoting cyber education initiatives that will help create a vibrant cyber workforce. States have made significant progress in recognizing that creating a robust curriculum in Science, Technology, Engineering and Math (STEM) and Science, Technology, Engineering, Arts and Math (STEAM)[1] can help meet the growing demand for cyber professionals. While states recognize the importance of growing a cyber workforce by expanding education opportunities beginning at a young age, funding and staffing for these opportunities at all levels of schooling appears to be a barrier to widespread implementation.

On the training side, almost every state offers online training materials that teach cyber "hygiene" and identify security risks for which employees and the general public should be aware[2]. Cyber training and education for state employees is voluntary in most states, but at least 13 states have made it mandatory.[3] Rhode Island's Cybersecurity Commission looked at the resiliency of the state's digital networks and recommended that it roll out "system-wide training to all state employees on cyber hygiene—focusing on spear phishing in particular."[4] California sends out phishing links to staff that, if clicked, will lock the employee's computer and require the employee to undergo training before he or she can regain access to online state systems.

Linking sound cyber policy to state economic success is a theme in education and workforce development efforts. With this in mind, states are developing education pipelines to encourage young people to enter the cyber field and have passed legislation to foster this goal. The Colorado legislature passed a bill, H.B. 1453, which was signed into law in May 2016. The new law combines comprehensive cybersecurity goals with an appropriation of funds to implement these goals and recognizes that Colorado is "well-suited to serve as a location for comprehensive cross-sector and interstate strategy to support … the education and training needed to prepare government and private sector leaders to respond to … attacks."

This legislation acknowledges that it is in the state's best interest to form strategic partnerships with state universities such as the University of Colorado and community colleges, and to coordinate "the

[1] NCSL STEM research

[2] State Cybersecurity Training for State Employees

[3] States that require cyber training for state employees include: Colorado, Delaware, Florida, Maryland (where state agency personnel have to take a cyber class each month in order to gain access to state networks), Montana, Nebraska, Nebraska, North Carolina, Ohio, Oregon, Pennsylvania, Utah, Virginia and West Virginia.

[4] Rhode Island Cybersecurity Commission Framework

development of elementary and secondary education feeder programs." It also creates a Colorado Cybersecurity Council, which appoints members from public safety, treasury, state information technology (IT), public utilities and higher education to make recommendations? It calls for establishing or expanding cyber higher education programs with a revenue source to support this expansion. Finally, the legislation establishes online courses, training and academic symposia for government leaders at all levels.

The Maryland legislature passed legislation (S.B. 542, Ch.358) in 2015 creating its Cybersecurity Council. In an Interim Report, published in July 2016, the Cybersecurity Council stressed the importance of cyber education and early engagement of students beginning at in middle school. Maryland has attempted to spark interest in technology careers in younger kids through summer camp programs. Older students are encouraged to pursue cyber careers through tuition-for-service programs and Maryland's Cyber Pathways Program, which fast tracks training in IT/cybersecurity and is offered at 14 community colleges.

Created by a 2015 executive order, Rhode Island's Cybersecurity Commission committed to assessing the state's current cybersecurity workforce development and education activities. The commission's goal is to determine barriers to expanding workforce and business development opportunities, and provide recommendations to eliminate those barriers. Currently, several Rhode Island colleges offer cyber tech/policy degrees, cyber courses, or network and system administration certifications that can be used to feed into a four-year college program. High schools are encouraged to participate in "CyberPatriot," the National Youth Cyber Education Program's annual national cyber defense challenge coached by experts in industry and academia.

Texas has also participated in the CyberPatriot program as a means to "give hands-on exposure to the basics of cybersecurity and inspire students in this critical and growing field."[5] Texas also identified the need to increase the number of cyber professionals in the state by investing in higher education cybersecurity programs and creating a "comprehensive cybersecurity pipeline through the BETS partnership (Business Executives for Texas Security) to introduce cybersecurity initiatives from kindergarten through graduate school programs.

Virginia held extensive hearings and conducted research through its Cybersecurity Commission to examine ways to create a networking and cybersecurity career "ecosystem." The system maps a career path, from entry level computer networking and support to advanced networking and then to cybersecurity careers. Virginia enlisted the assistance of the private sector to determine what type of jobs lend themselves to an eventual transition to cyber careers. Before concluding its work in March 2016, the commission was briefed on the demographics within the state to identify the level of need for cyber professionals.

Securing state digital networks traces back to reducing human error and the need for basic cyber skills education for state employees. Economic growth is linked to sound cyber policy and strong long-term investments in education and workforce training. By improving state employee awareness of cyber risks on the job and creating sound curriculum in state schools and universities, states are systematically addressing the growing needs in this area.

[5] http://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=68.