Please review our public comments for

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development

https://www.federalregister.gov/documents/2017/07/12/2017-14553/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure-workforce

Comments provided from:

Phil Bertolini, CIO
Chris Burrows, CISO

Oakland County
1200 N. Telegraph Rd, Bld. 49W
Pontiac, MI 48341

Growing and Sustaining the Nation's Cybersecurity Workforce

1. What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?

Internally we track the number employees trained for our User Awareness Training program. We also advocate that all IT departments continuously train their staff but do not strive to train a certain percentage of IT employees. The training is primarily based on our "Individual Development Plan Program" for each employee.

Five Southeast Michigan counties and the State of Michigan created the Cyber Security Assessment for Everyone or CySAFE. CySAFE is an assessment that provides an end user the ability to rate themselves against 36 controls originating from NIST, ISO and the 20 Critical Controls. The rating will then help produce a to-do list that is prioritized for the end user's stakeholders. CySAFE can be downloaded by public entities at no cost at www.g2gmarket.com. Simply starting with the CySAFE assessment will instantly provide a set of metrics to measure the foundation of a cyber security platform. Training end users and IT support staff are included in the CySAFE measurements.

2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

All organizations have different RACI models when it comes to IT security. Some organizations are updating their job descriptions to include specific IT security responsibilities. There is a disconnect between HR and IT when it comes to work roles, knowledge requirements, abilities and compensation for IT security professionals.

Current technology classifications, both private sector and public sector, may not map to the current staffing needs for cyber security. A more standardized approach to these classifications would assist everyone nationwide.

3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

We, Oakland County Michigan, have the proper policies in place and we have a very active security team managing our cyber presence. We hired a CISO several years ago and each year built a staff underneath him. The policies are regularly enforced and audited to ensure we are as safe as possible in the ever-changing threat landscape. We currently educate the 4000 + staff each year through computer based training.

As we discuss these issues around the State, we find that most organizations have limited cybersecurity policies if any at all. Those that do have policies have a single ITSEC policy and conduct an annual User Awareness Training program. Very few organizations send their IT staff to specific ITSEC courses. Many do not train their internal entity wide staff.

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (*e.g.*, energy vs financial sectors)?

Employers need passionate, driven-to-learn, problem solving, logic oriented and customer focused workforce. Employer expectations are realistic because those are the skills needed to be successful. This is no different for a cyber security team. The difference is that a cyber security team must dig in and review the work of their peers which can sometimes be controversial. Executive leadership must be prominent or the business units could overrun the security staff by being passive aggressive.

Sectors do not matter as much as the combination of all the skills. Most organizations need to focus on the core controls of cybersecurity: patch management, account/password management, training, backup/recovery, inventory management and incident response. Cyber Security is an effort that requires perseverance to break through the many roadblocks placed in the way. Those staff that do not have the ability to break through should not be part of a cyber security team.

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

In our experience, we found that SANS offers classes that are up-to-date and relevant. Skills learned over the week-long class, can be used immediately. The instructors are ITSEC experts

and have excellent teaching skills. There are other training opportunities available but SANS provides the most benefits.

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

The battle to train internal and external people is difficult. We are only as prepared as our weakest link. Most of cyber-attacks have a "people" component so training becomes one of the most important defense tools. Low cost training opportunities must be consistently made available to all levels of government no matter what the size.

Another issue impacting training is that there are very few ITSEC university programs. Most current ITSEC employees started in another IT role (System Admin, Network admin, developer, PC support). The SANS courses are valuable but expensive ($5-6,000 for a six-day course) plus travel. Many companies cannot afford to send many staff to SANS courses.

7. How will advances in technology (*e.g.,* artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?

The advent of IOT and AI have provided another significant challenge for government. Governments are judged differently than the private sector when it comes to cyber intrusions. The private sector can handle cyber issues with much less fanfare which puts government officials square in the crosshairs of the public. Providing services with devices that currently have limited security features may pose too much of a risk portfolio for most government IT leaders. The federal government could play an important role in diagnosing the appropriate cyber controls for both IOT and AI. However, the growth of IOT is happening faster than organizations can adapt to AI. ITSEC employees are needed to analyze patterns and decide on what actions are needed.

8. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:

i. At the Federal level?

The federal government could play an important role by strengthening the adoption of the NIST standards within the state and local governments. They could also provide low cost or no cost consulting for local governments to assist in securing the proper training. Utilizing the federal buying power to assist local governments access to low cost resources such as templates/how-to guides, technical and user training by leveraging the buying power of the federal government to access discounted tools that would help the state and locals implement basic security controls. This would save limited dollars available at the state/local level by avoiding having to purchase these individually or having to contract privately for these services. ii. At the state or local level, including school systems?

Promoting cybersecurity careers early in the educational track (middle school/high school); Offering internships; Creating an environment for students to get "free training" or "discounted university classes" if they work in the public sector for three years (or a specific amount of time); Creating an atmosphere for learning and making cybersecurity a priority within state and local government. The younger generations have a desire to make a social impact which can be obtained in the public sector much more than in the private sector; The "social impact opportunity" could be a strong marketing tool to drive growth in our cyber security workforce.

Finally, the State could ensure that the bulk of federal cyber dollars make it into the hands of the local governments. Too much of the funding is held by the States for their use or overhead.

iii. By the private sector, including employers?

Awareness, awareness, awareness. The private sector has a responsibility to protect the citizen's data just as much as the government does.

iv. By education and training providers?

Keep the training opportunities affordable and easily distributed.

v. By technology providers?

Too many providers have been implementing software with security holes that could prove to be disastrous. As governments implement COTS software it has been incumbent upon the governments to find security holes. Providers must effectively test their products and make the appropriate changes before they implement in a government environment. There have been too many breaches where default passwords have been left in place or the code for a system has openings for attackers.

Kevin Kimball,

NIST Chief of Staff.