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

General information

The Computing Technology Industry Association (CompTIA) is the world's leading not-for-profit information technology (IT) association. With approximately 2,000 member companies, 3,000 academic and training partners, over 100,000 registered users and more than 2.4 million IT certifications issued, CompTIA is dedicated to serving the tech industry and tech workforce through education and training programs, market intelligence, social innovation, and more.

CompTIA supports the current NIST cybersecurity workforce and is committed to ensuring they have the necessary tools and knowledge to keep us secure as a nation, while also supporting policies that will help to strengthen the workforce of the future. Among other things, which we have outlined below, we support enhancing the use of industry-recognized credentials, modernizing the way we teach and train, and improving the sharing of information between industry and government.

CompTIA is an advocate for the tech industry and tech workforce in various governments around the world. Our work continues in the form of apprenticeships, mentoring, and offerings designed to educate the workforce to meet the ever-expanding cybersecurity threat landscape.

CompTIA recognizes that while progress has been made on many cybersecurity fronts, there is still much work to do. CompTIA welcomes the opportunity to support efforts, such as this NIST initiative, to continue to work towards viable, measurable, and scalable cybersecurity workforce solutions.

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?**
   There are several important streams of data needed to effectively evaluate and track the growth and sustainability of the Nation's cybersecurity workforce:

   a. Cyber workforce dynamics
   b. Cyber readiness
   c. Training / performance effectiveness
   d. Return on investment

   Cyber Workforce Dynamics

   Cyber workforce dynamics covers the data associated with understanding the "who," "what," "where," and "how" of the cybersecurity workforce. While the U.S. Bureau of Labor Statistics and related agencies involved in collecting and aggregating these types of data points provide a good starting point, their output lacks granularity or simply does not exist in a number of critical areas.

Many industry groups conduct surveys and research to help complete the picture. For example, CompTIA in partnership with Burning Glass Technologies and NICE, launched www.cyberseek.org during late 2016. This first-of-its-kind supply/demand heat map provides new insights into cyber workforce dynamics. While these efforts are a step in the right direction, opportunities remain for additional macro-level work.

Cyber Readiness

In evaluating cyber readiness, a critical question to pose is whether cyber readiness of our nation's private sector and public sector institutions follow a classic bell-shape curve? Or, does it skew towards a higher concentration of ill-prepared organizations? Where are we today, and based on that baseline, what are realistic improvement milestones over the next decade?

Data wish list idea: to answer these questions, seek an add-on component to an existing government research study (e.g. the Economic Census) or possibly a new dedicated vehicle for collecting cybersecurity data

A number of industry groups and companies have created assessments or tools that attempt to address this question, but there are often gaps in coverage, shortcomings in the assessment itself, or other limitations.

Data exploration idea: is there a better way to assess cyber readiness?

Training / performance effectiveness

It would be helpful to know what the optimal way to assess training effectiveness and how knowledge gains translate to workplace performance. Given budget constraints, time constraints, and opportunity costs, we suspect return on investment variables impact the calculations of employers and workers. Given that cybersecurity is viewed as a cost center by most business leaders, we should explore what metrics are needed to shift this mindset.

Like many across academia and industry, CompTIA has wrestled with these thorny issues. For example, CompTIA led a data sharing exchange pilot in Illinois in a quest to determine if an IT industry-recognized credential helped boost a community college graduate's employability and income potential. The findings were significant:

- Certified students had slightly higher employment rates than did non-certified peers.
- Certified students had substantially higher earnings – about 30 percent higher in the exam quarter and nearly 50 percent higher by the third post-exam quarter.

- The employment and salary "gap" between certified and non-certified graduates widened as time went on.[1]

It is clear that the return on investments for certifications are worthwhile and is something that should be further analyzed.

Data wish list idea: expansion of the CompTIA pilot and similar efforts to quantify training, job performance, and ROI.

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

CompTIA supports the NICE Cybersecurity Workforce Framework. We believe it sufficiently captures the workforce categories, specialty areas, work roles, and knowledge/skills/abilities of the cyber workforce. From CompTIA's perspective, the NICE Framework appears to be making gains, with greater numbers of organizations using it some capacity. While there is certainly room for improvement in promoting understanding and agreement, NICE Framework initiatives are headed in the right direction.

One possible area for evaluation is the mechanism for incorporating new workforce categories, specialty areas, work roles, or knowledge/skills/abilities. Given the dynamic and rapidly evolving field of cybersecurity, we believe it is critical to anticipate how emerging trends, such as artificial intelligence, could impact the NICE Framework and quickly respond accordingly.

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

CompTIA has long championed the need to make routine training a part of an organization's overall cybersecurity policy. According to CompTIA research, human error is the primary culprit behind many security breaches. Furthermore, the research reveals that just 1 in 5 businesses feel that their current level of security is completely satisfactory.[2] This sentiment is relatively consistent across companies of different sizes, though there is some difference based on job role. IT staff tend to view security more positively than business staff, perhaps due to a more technical view of security rather than a view that includes policies, processes and employee awareness.

Appropriate cybersecurity policies include requiring continuing education for all employees. This includes "end user" training, as well as education to ensure that IT professionals can meet the challenges they face from changes in today's infrastructure, as

[1] http://www.creatingitfutures.org/docs/default-source/PDFs/data-sharing-whitepaper.pdf?sfvrsn=2

[2] The Evolution of Security Skills (attached), CompTIA Research Report, April 2017.

well as the ever-changing cyber threat landscape. It is not enough to simply use training as an informal incentive to attract or keep IT talent. Continued training needs to be part of a company's stated security policy.

For non-IT/cybersecurity employees, we point to CompTIA's CyberSecure. This is a self-paced training course that teaches employees how to follow security practices vital to protecting any organization. The 60-minute training focuses on situations relevant to everyone from the receptionist to the CEO.

Enforcement of workforce education can be greatly simplified by working closely with organizations that reflect the needs of the industry. CompTIA, for example, provides an extensive Continuing Education (CE) program[3]. This program has been in place for more than seven years. It has been adopted by various entities within the United States Department of Defense (DOD), as well as by contractors and individuals around the world. Such programs are designed to reflect the needs of the industry. It is vital that certification organizations create programs that are thorough and comprehensive. These programs should also be designed to encourage continual learning on the part of individuals so that they do not allow their skills to lapse.

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)?**

Several variables are at play in determining employer needs for cybersecurity knowledge and skills. Consider:

- Segments of the market "don't know what they don't know." While there are a higher proportion of small and medium-size business that fall into this category, there are also plenty of large organizations that have a legacy security mindset, leaving them underinvested in emerging cybersecurity skill sets. Relatedly, segments of employers that lack a true understanding of their workforce needs may fall into the trap of "asking for the world" from prospective candidates, resulting in disconnects.
- Segments of the market have a reasonably good idea of what they need, but cannot get there. This could be a function of pipeline or skills gaps, but also resource constraints. Most SMBs will not be in a position to afford highly specialized cybersecurity talent. There are options to overcome this, such as working with a managed security services provider (MSSP), but that still requires a degree of IT sophistication and budget.

Circling back to the questions above, ideally, employers are thinking holistically and strategically about their cybersecurity workforce needs. Of course, this is easier said than done. Tools such as IT roadmaps and frameworks, such as the NICE Cybersecurity

[3] https://certification.comptia.org/continuing-education

Workforce, are a good starting point. At the same time, it can be overwhelming for small businesses or industry verticals that have not historically been heavy users of technology. We recommend that the Small Business Administration partner with industry to put out of set of "best practices" to help these organizations navigate these waters.

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?**

   The most effective programs are based upon industry-accepted IT workforce skills-standards based on IT job roles. These programs are taught by prepared and qualified instructors with related degrees and certifications, they use hands-on labs, and they always finish with an assessment tool to validate knowledge, skills and abilities (KSAs).

   However, improvements are needed for the effectiveness and scalability of cybersecurity education, training, and workforce development. Effectiveness can be met through hands-on training and assessment. Scalability can be met through cloud-based cybersecurity training, but a problem exists. At this point in time, cloud-based solutions tend to be expensive.

   Traditional certification and brick and mortar training can only reach a certain number of cybersecurity professionals. There is a need for more options including low-cost cloud-based cybersecurity training and assessment tools. We are committed to working with industry, government and academic partners to explore a broader range of solutions to achieve effective/scalable cybersecurity, education, and training.

6. **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)?**

   Things are changing rapidly when it comes to technology. There are a few opportunities for us as things continue to evolve. First, it is for us is to more completely train individuals of all generations on how today's end points operate. It is not enough to be an excellent consumer of these devices. It is vital to understand the internal workings of these devices and their software. This type of understanding makes it possible for security workers to anticipate issues.

   Secondly, we should highlight tracks of instruction that properly educate individuals concerning today's modern infrastructure. Too many organizations rush into teaching workers about advanced cyber and physical security concepts without first grounding those individuals in advanced infrastructure issues.

For example, we are seeing interesting developments in the growing field of security analytics. The Security Analyst job role involves filtering all network traffic in real time to find bad behavior. It is a newer cybersecurity skill set that all IT cybersecurity professionals need as we are now rapidly moving beyond the need for traditional "blocking tools" such as anti-virus software.

7. **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?
ii. At the state or local level, including school systems?
iii. By the private sector, including employers?
iv. By education and training providers?
v. By technology providers?

CompTIA continues to work closely with each of the sectors discussed above. For a decade, we have been a *de facto* education standard for the United States DOD 8570 initiative. Lately, we have introduced the cybersecurity pathway[4] to ensure that individuals are properly trained in all of the latest technologies the Federal Government has been charged to secure. We continue to work closely with civilian departments at the Federal level. These organizations continue to see the need for assessment-based training. Now that the 8570 initiative morphs into 8140, we encourage Federal organizations to consider the sophisticated training and assessment solutions that exist. Not everyone provides the right mix of hands-on education and performance-based assessment. But it can be found.

We need to implement training that has a valid, industry-respected assessment approach. Otherwise, it will be impossible to objectively verify if individuals have truly internalized their learning.

We encourage a unified approach to education in the United States. Apprentice programs are one such approach. They continue to have impressive results throughout the world, including the United Kingdom. For decades – if not centuries – educators, governments, and corporations have worked in isolation. There have been benefits to this approach. For example, corporations have been able to focus on practical cybersecurity implementations, where academic institutions have been able to look forward and conduct cutting-edge research.

CompTIA supports the recently introduced legislation entitled "The CHANCE in Tech Act." This legislation will ensure that quality candidates are recruited and provide compressed and targeted training to meet specific employer needs. Additionally,

[4] https://certification.comptia.org/it-career-news/post/view/2016/10/11/introducing-the-comptia-cybersecurity-career-pathway

secondary schools will be recognized for ensuring their classrooms are teaching the necessary skills for students to compete in the 21st century workforce.

To create tomorrow's workforce it is vital for each of these sectors to work more closely together than ever before. One way to do so would be by adopting industry-standard education programs and by working closely with each other through high quality, high-impact outreach programs. These programs can include roundtables and sessions that create education programs. Internships are just one step to take.

We encourage ending programs that are not based on industry-standard best practices, or which focus on vendor-specific implementations. It is also important for the Federal Government to focus on training that can provide proof of candidate improvement. Therefore, it is vital to continue an emphasis on programs that can provide metrics-based education. Metrics can include:

- Ability to set network baselines.
- Creation of proper traffic and cybersecurity thresholds.
- Creation of alerts.
- Custom configuration of SIEM tools to model network attacks
- Reduction of "dwell time" (i.g. the time between a detected event and when the attacker has been neutralized)
- Ability to recover quickly from attacks.
- Creation of network resilience procedures and steps.
- Reduction in Single Loss Expectancy (SLE) and Annualized Loss Expectancy (ALE), as tied to training and assessment.
- Increased ability to complete projects.
- Ability to pass industry-standard assessments and exams that act as a capstone to training.

We appreciate the opportunity to weigh in on strengthening our cybersecurity workforce, something that is always of top of mind to us as an organization. CompTIA is committed to continuing to work with our government partners to strengthen our current workforce and ensure that we are on the right path for creating the workforce of tomorrow.