WORKSHOP ON CYBERSECURITY WORKFORCE DEVELOPMENT

August 2, 2017

NOTES FROM PANEL DISCUSSIONS

Table of Contents

INTRODUCTION

Steven Koch, Deputy Mayor, City of Chicago

- Computer science is a graduation requirement in the public school system
- Partnership between community college and DOD, and another with the military

PANEL 1

MODERATOR: Adam Sedgewick

PANEL MEMBERS: Tim Herbert (T), Matt Loeb (M), Will Markow (W), Debbie Sagen (D)

QUESTIONS

1. **How to determine current demand for current workforce demand? (What exactly is the present workforce demand for cybersecurity jobs?)**
   - First need to define what cybersecurity is: (burning glass) captures all core information security workers/analysts, as well as those who are "cybersecurity enabled" (software developers, people who do 30%+ of job in cyber) (W)
     - Build a relative measure of supply to demand – there are less than one cybersecurity workers available for every one available opening
     - Improve job matching and the available tools for closing the gap
     - Most cybersecurity jobs are now outside traditional roles
     - 10-15% of the entire IT workforce encompasses cybersecurity
   - NICE Framework categories of Operate and Maintain and Securely Provision are the most in demand cybersecurity positions
     - skills are across IT – about 2/3 demand for skills are now outside of traditional cybersecurity roles
   - People are the number one capability, as well as the number one vulnerability (M)
     - Cyber is a new domain that encompasses air land sea and space
     - The number AND quality of the people that are required is the issue – we need to think more expansively… what can we do with the workforce today to channel people into available jobs TODAY
   - Representatives from private sector cybersecurity employers do not answer questions, so we (educational institutions) guess about what is needed (which is causing the misalignment) (D)
     - Contractors post the same job position and projects multiple times, which means trainers are grossly over estimating the need

2. **What are employers doing to help address the gap? (How do employers define their workforce needs? Do they use job titles, position descriptions, duties, qualifications, etc., that are standardized or easy to measure?)**

- Employers are looking in two directions: (1) we want ones who will show up, be creative thinkers, and we can teach them the rest (forensic cyber); (2) those who have very specific needs based on industry credentials specifically spelled out in contracts. (D)
    - A Bachelor's degree may no longer be the gold standard, and employers are seeing this
- Employers may not know which bucket they need to fall into; they may not know what they need (W)
    - 8 out of 10 employers say a 4 year degree does not adequately prepare people for cybersecurity jobs, yet 8 out of 10 jobs request it – here is a disconnect
    - Organizational bureaucracy or politics may be to blame for the disconnect; it's not necessarily that HR does not know what they need
- Smaller organizations cannot afford to hire what they really want – something very specific. They hire someone who can be a jack of all trades (T)
- Many applicants are not familiar enough with cybersecurity to even understand what job they are actually applying for (M)
    - The credential doesn't matter as much; they want them to have actual hands on work
    - How can we look at workforce development as "retraining" those who are currently in the workforce instead of only focusing on the young ones who are coming up
    - Took people who were from non-technical careers, put them through a skills training program to see if they actually could be taught these new skills – and they were able to reskill them
    - We need to also invest in those who are not the likely choices
    - 55% of respondents say that the qualification isn't the degree/credential, it's whether the applicant has practical hands-on experience necessary to help them complete their job functions.
    - We may need to think beyond the educational system of today; we need to look into retraining people who are already in the workforce
    - UK Skills Training Program Study ($1.2m)- Wanted to see if you can instill skills in individuals to fulfil job requirements – conclusion – studied 55 people and discovered that it is possible to re-train them in cybersecurity and for them to be successful
    - Need to strengthen workforce development efforts to create opportunities for people who have the capabilities of performing cybersecurity jobs but come from different fields, and re-train them for the field.
- Federal government needs to play a bigger role in training our talent
    - The younger generation of today isn't just motivated by money; they are also motivated by training opportunities/professional development, which government can provide.

3. **What should we be doing to influence supply and demand, and what should we be doing for the next phases? (What is the government role to influence workforce supply and demand as well as to shape both organizational, sector, and national workforce planning?)**
    - Map certifications to NICE framework (T)
        - Some of the work roles are far too specified for small business companies
        - How do we incorporate non-cybersecurity specific roles into this?
    - Security needs to be part of the fundamental curriculum (M)
        - The need for hands on training (cybersecurity is comparable to airline pilot). But are we training them enough for the unknown?

    - Traditional credentialing method will not work for cybersecurity – sit around and read and then take a test
- The federal government will continue to play an important role (D)
    - Developing the NICE Framework – how to talk about it and how to implement across agencies
    - Center of Academic Excellence (CAE) – the seal of approval
        - Challenge: unfortunately, does not yet show a measure of quality; it rates the curriculum, but does not tell anything about the number and quality of the students coming out of those schools
    - Cannot find teachers with the credentials needed to teach the students – they get paid way more in the private sector than the educational system can compete with
    - Internships/apprenticeships: work-based experience is crucial and this helps new students in this field bridge the gap
- CYBERSECXP (ISACA Credential) (M)
    - There are so many credentials out there that there is credential confusion; we need to figure out how to standardize and organize
- Government has a role of a convener, as well as a role of a consumer (W)
    - The federal government is the largest employers of cybersecurity professionals in the country, therefore needs to play a role in developing best practices (is more likely to hire people without degrees, and therefore plays a role in bridging that gap)

4. Relationship between information technology and operational technology

- at the college level, look across all disciplines to help develop specific modules in EACH area specific to that discipline (D)
    - the ENTIRE workforce needs to be able to respond to a cybersecurity threat
- what are we doing to build up organizational capability, and are we being realistic? (M)
    - We still need people at the macro level, not just people at the specific level
    - Use of capability maturity model
    - The type of threat experienced by each industry differs
- IT has a disruptive force as it evolves – traditional roles are becoming hybrid roles, which is creating new challenges for the training community; their training programs which traditionally worked no longer do, and they now need to try to figure out how to combine programs to ensure that they are adequate (so that they do not lead to the development of an even larger skills gap than we already have). (W)

PANEL 2

MODERATOR: Steve Casapulla

PANEL MEMBERS: Art Conklin (A), Tom Fleming (T), Lazaro Lopez (L), Scott Nelson (S), Jeff Pike (J), Tom Polak (P)

OPENING COMMENTS:

- army reserve cybersecurity initiative
- we are able to certify kids in high school; it's getting them into the workforce that is our new challenge

1. **What strategies/approaches are currently being used to build the workforce, and are they sufficient?**
    - Offer programming classes as a way to get them interested (hardware and software) (P)
        i. Find the kids who are interested and give them other opportunities to develop (i.e., competitions)
        ii. A lot of kids are qualified, but no one hires a 16 y/o
    - We fund things that are important to us (A)

2. **What can be done to more rapidly grow the cybersecurity workforce needed by employers?**
    - We lack a vision from the government on how to move forward (implementing the plan). Quality? How do we build a pipeline in the communities
        i. We need to make sure there is solid communication across partners (academic says government and private sector don't hear them, etc.)
    - Aptitude assessment – identify people who have the ability to do the work (J)
        i. What is the shelf life of cyber skills? Not long, so people need to be continually relearning

3. **What are the roles/purposes of the education vs the training/retraining of people?**
    - Must meet individuals at each touch point (i.e., as elementary school, entry level incentive credentials) (L)
        i. What is the value for each person at each level to make the investment into becoming a cybersecurity person?
    - Training without education will not work (A)
        i. The training will get you a job on the technology that is available now, but that technology will change, and then you will no longer be relevant
    - The jobs (and associated skills) need to be mapped better to the credentials – you cannot get mad at the employee if they cannot do the job you want if they have a credential that does not map to the job (J)

- Look at a different model (S)
    i. Look at other countries for their model
    ii. A key problem is that we are creating competing programs
        1. This is where the government comes in and plays a key role to consolidate and set standards

4. **Regarding education and training, where do we find the trainers? (What is the relative role and purpose of education (K-12, community colleges, universities) versus training (leading to industry-recognized certifications) to build the Nation's cybersecurity workforce?)**
    - Line up partners who do have the capacity (S)
        i. How do you build the community around the teacher? (i.e., companies) especially for high school teachers. Set up so the companies are investing in the teachers and are investing in their own solutions to the problems they are facing (since they are investing in developing the workforce which they will then employ).
    - Develop pathway programs for those coming out of their career (A)
        i. Need to find ways to entice teachers in

5. **How do we set expectations for entry level jobs for students and those looking to transit mid-career, as well as for the companies?**
    - Get people to understand the possibilities that lay in cybersecurity and IT (S)
        i. Try to get rid of the social stigma associated with being a "cyber geek"
    - Tell students more about what each job entails, because they do not know (do more career planning) (P)
        i. Get kids exposed to the different skillsets (create clubs) so they get exposed and will explore those career paths
    - Use models already available ("incubators to you") (L)

6. **How do we find, train, and prepare women and minorities?**
    - Target universities and high school students (S)
        i. What are the opportunities? We need to provide scholarships
    - The younger generations are where the diversity is (A)
        i. If we want to fix things, we need to fix our base

7. **Although we have a lot of events and competitions, how do we develop in cyber the non-technical or hands on aspects of it? (policy, legal, architecture, etc.)**
    - You cannot do the technical part if you do not have the soft skills – if you cannot explain the tech to a non-tech, they will not invest in you (S)
        i. The psychological impacts are just as important as the physical impacts
    - It's not about school, it's about a career path (A)
    - Our schools only focused on test taking, and we need to consider working away from that and giving students more realistic chances to prove themselves (L)

CLOSING COMMENTS

- cybersecurity is cross sectional; we need to develop a workforce that is representative of this (T)
- summit this fall in Illinois (schools) (L)
- "never let a crisis go to waste"; make it so these trainings can be translated into years of credit for a 4 year degree for those who need to get a 4 year degree (S)
- the employer needs to do their due diligence to make sure that what they are asking for actually maps to the skills for the job they are asking to be done (J)
- develop a resource to direct students to school institutions to get the skills they need; have a national body that says "here are the leading industry training organizations to develop these specific skills" (P)

PANEL 3

MODERATOR: Kim Holden

PANEL MEMBERS: John Germain (J), Jason Hite (H), Laura Loiacono (L), Ted Mims (T), Ray Trygstad (R), Jason Volmut (V)

1. **Given the shortage of cybersecurity talent, what sort of recruitment mechanisms/tactics should be utilized?**
    - need to find the right fit for the company (J)
    - there's a disconnect in the HR community on how to assess the cybersecurity talent pool (H)
    - told to go to USA.gov and download app and apply on the spot (L)
        i. "You all are saying there are so many jobs available out there, but I can't even figure out how to apply or where to look;" it's using the same process as all other government agencies
    - work with schools to recruit into the schools first, and then try to recruit into the workforce – recruitment into cybersecurity workforce starts in the schools (T)
        i. We are sitting here saying that there is a critical shortage, yet here is a PhD who is getting shut out if she can't apply in the first 20 minutes
    - Big disconnect between the training part and the hiring part (R)

2. **How can existing employees be retrained to go into cybersecurity, and how do you suggest doing that?**
    - This is the best pool to look at (J)
        i. Needs to be a certain kind of person: likes solving puzzles, can stay calm and focused

3. **What skills as an employer do you value for a cybersecurity employee?**
    - gamers; strategic multiplayer online gamers (V)
    - need to be able to solve problems (T)
    - Is the problem that we are defining "solving problems" from a purely mathematical and logic sense? what about those who are complex and abstract thinkers? Are they being washed out?
    - strong writers; those who can write better do better. (R)
    - how are you identifying these people through there CVs? How do you find a problem solver based on their CV? (L)
    - running a multibillion dollar company means I am looking for qualified, experienced people who can come in and fix things now; I can't afford to spend time on people who I need to train on the job. (J)
    - HR needs to change from being a gate keeper to being an enabler (H)

4. **Diversity: what do u think can be done to increase the number of women and other diverse candidates into the CYBERSECURITY workforce (including older individuals)?**
    - a cultural change is needed in order to recruit more women (V)

5. **Are resumes an ineffective tool? What type of innovative tool would you use to showcase your skills?**
    - A cyber challenge that gives you a score and puts you in a queue given your score, and then you can go back and submit your resume. Or a nationally generated challenge that changes ever 3-6 months with a score? Maybe like the SATs; a challenge generated by a specific company that has a testing center that can verify you're taking the test, then the individual enters a secure area and completes the challenge, and is then given a score which can be forwarded to the cybersecurity program of the individual's choice.

6. **What is the best strategy for retaining employees with the skills you want?**
    - You have to invest in them; need to make a connection between them and the company so they become invested (J)

7. **How can we improve the understanding of cybersecurity for managers?**
    - Education (V)

8. **How can we teach people to tackle hard problems?**
    - Build out robust training systems (R)
        i. Give them attack simulations so they can practice

PANEL 4

MODERATOR: Christine Quinn

PANEL MEMBERS: Shannon Donahue (S), Gabrielle Helfgott (G), Nicholas Bruno (N) *[replaced Emilio],* Samit Khare (K), Drew Morin (D), John Sands (J)

1. **How do you decide to recruit from outside or within (train those who you already have)? And does organization size matter?**
    - Allow employees to grow skills and cross train by providing internal internships (D)
    - Develop an assessment tool for managers to test employee's actual skills and can see where the strengths and weakness are (helps measure day to day performance)

2. **How do you decide if someone needs additional training?**
    - use 360 degree reviews (D)
    - "harmonization of skills" -> what are the typical skills needed for a specific position in your organization (K)
        i. What are the gaps in the skills of my current workforce?
    - align academic and industry sides to make sure they are teaching what is needed (J)
        i. Create virtual environments for students to work in
        ii. Field trips
    - Cobalt program (cyber range) (D)

3. **How are you engaging employers and education together? Are employers finding employees who are prepared coming out of school?**
    - if an employee is not able to perform, the COMPANY has done something wrong in the hiring process (K)
        i. Cybersecurity simulations should be used during the hiring process
    - have employers invest in the employee by sponsoring the certifications (N)
    - competitions are particularly important to ensure that employees are skilled (J)

4. **How are apprenticeships being used in cybersecurity?**
    - Cybersecurity is much more like the medical field (D)
        i. Residency-type programs should be implemented where more complex thinkers can work side-by-side with SMEs to learn how to handle these kinds of problems

5. **What type of training have you identified as something that needs to be continually refreshed?**
    - Wireless technologies (J)
    - software defined networks; watch what's coming out of Def Con and Black Hat (D)

6. **Are there things you incentivize employees to do? (i.e. training)**
    - What really matters: (K)
        i. Focus on providing opportunities of learning and providing new challenges
        ii. New hires want to know the larger picture and where they fit into that; communicate this
    - they want to feel like they are contributing to something larger and are giving back (G)
        i. For millennials, work and life is blended
    - millennials will move around 3-5 times in their life; each time they move we are making the cybersecurity workforce as a whole better (D)

7. **Where are we in awareness of cybersecurity? How important is awareness in regards to cybercrimes and cybersecurity?**
    - Doing cybersecurity for compliance (K)

8. **Is there a role for research in defining future technologies?**
    - you need problem solvers and centers that can disseminate (J)
        i. "innovation" or "emerging technology" schools
    - we need to focus more on resilience (D)
    - block chain will become the new internet (K)

Closing comments

- Retention is important, especially given how fast cybersecurity changes (N)