1 - WORKFORCE DEVELOPMENT

Summary

Careers in cybersecurity are some of the fastest growing and highest demand job opportunities available. The U.S. Department of Labor (DOL) groups cybersecurity specialists within the category of "Information Security Analysis, Web Developers, and Computer Network Architects". The outlook for this group is promising. DOL expects 22 percent growth within the next decade, which is considered faster than average. Demand for information security analysts is expected by DOL to be "very high". They justify this by pointing to the increased frequency and sophistication of cyber-attacks. Based on these expected workforce requirements, survey questions were formulated to understand the needs of different entities in Missouri.

The survey questions developed for workforce development are the following:

1. What are the strengths employers see in current cybersecurity professionals and what are the weaknesses that employers wish addressed?
2. Would you utilize a cybersecurity institute in the state of Missouri that offered certifications for your employees? Would you find benefit if they offered directive communication for handling current threats, and networking opportunities with other businesses about cybersecurity?
3. How much are internships/co-ops experience important before joining the workforce? Do the companies have internship/co-op programs?
4. What are the preferred methods of educational/training delivery, i.e. distance streaming video, offline training, on campus training, site-specific courses, massive open online courses (MOOC)?
5. Which security certifications do employers seek in a cybersecurity professional? How important are those certifications to employers?
6. How can industry participate in competitions from K-12 to college?
7. What programming languages are necessary in your workplace that are not being currently offered in the education system?

Based on the survey results, discussions amongst subject matter experts, and guidance from other major organizations, the following gaps were identified with the recommendations.

Gap #1: Centralized structure for educational outcomes

Surveys and analysis by the team indicated there was a lack of cybersecurity awareness and available cybersecurity talent at all levels in many organizations. When talent is available, many organizations cannot afford dedicated cybersecurity professionals.

Currently, cybersecurity in the classroom is still maturing. While there are some great higher education programs across the state, they vary in focus. This can be confusing for students who want to choose cybersecurity as a career, as well as for businesses in Missouri that hire cybersecurity professionals directly out of college.

Academic Designations and Accreditations: Educational entities such as technical institutes, community colleges, four-year colleges, and research universities can provide Center for Academic Excellence standards as highlighted by the National Security Agency/Department of Homeland Security (NSA/DHS). These standards prescribe particular sets of topics on security and privacy that accredited institutions must deliver to specific audiences. The state currently has one Center of Academic Excellence in Information Assurance which functions at the graduate and professional continuing education level. The Computing Accreditation Commission (CAC) of ABET, Inc. is proposing to include cybersecurity as a specific part of the CAC Computer Science Program Criteria for four-year and above universities to follow who wish to be accredited. Apart from these, there is the cybersecurity education project that also attempts to frame an accreditation mechanism.

Research: The state has one Center of Academic Excellence in Information Assurance Research with additional research activities at other universities focused on cybersecurity research. The research activities at these schools can result in outreach to support state cybersecurity needs through federal programs such as the Industry/University Cooperative Research Centers (I/UCRC) which partner industry and government with research programs. It is difficult for industries to learn about research capabilities statewide and determine how this research capability can be used to assist specific cybersecurity issues. There are also few terminal degree granting universities in Missouri, which forces students to go to other terminal degree granting universities in other states.

Recommendation: Cybersecurity Institute

To address the gaps noted above, the establishment of a cybersecurity institute for the State of Missouri is proposed. This centralized body could serve as a partnership between education, industry and government to identify relevant training, research, information sharing activities and communication to help citizens identify relevant cybersecurity topics that people, businesses and organizations need. This institute thereby would act as a facilitator of cybersecurity related educational and workforce development endeavors between different entities within the State of Missouri. The different roles this institute would assume are:

Academic Coordination: The institute would provide a clearing house and expertise for those institutions seeking cybersecurity designations and accreditation. This is a challenging task and the existing accredited institutions can provide assistance through the institute to share best practices and facilitate developing curriculum that meets national standards.

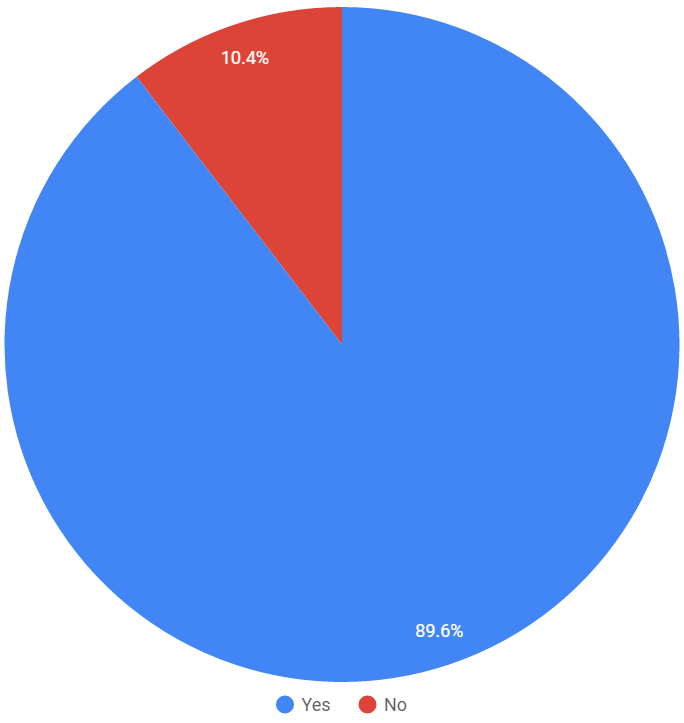

Figure 3: Survey participants that would utilize cybersecurity institute.

Research Coordination: The institute would provide "one stop shopping" for businesses and governments seeking solutions to cybersecurity issues. Federal support can enhance state support

through the Federal I/UCRC programs and others to bring together industry, education, and government.

Research Funding: This proposed institute would become the conduit to fund cybersecurity research in the state. State and national funding for cybersecurity topics is critical for researchers within the state of Missouri. This institute can become the facilitator between public and private entities to encourage research for the most pressing topics that impact the State of Missouri.

Scholarships: Another important role of such an institute would be to hand out scholarships to keep students in the state. This is an important undertaking since scholarships attract student's interest and provide incentives for high-achieving students to stay in the state. The National Science Foundation Scholarship for Federal Service (SFS) is a program designed to encourage bright students to pursue education and enter government service (both state and federal).

Career Services: This institute would also become a facilitator for industries that seek individuals to hire; everyone from interns to full-time hiring. Partnering with the Federal Office of Personnel Management (OPM), the SFS program virtually guarantees job placement. Apart from the different funding sources, state and national funding for cybersecurity topics is critical for researchers within the state of Missouri. This institute can become a facilitator between public and private entities to encourage research for the most pressing topics that impact the State of Missouri.

Gap #2: K-12 educational short falls

In today's society, cybersecurity continues to be a growing concern. From the individual to corporate perspective we are all seeing an increase risk of intrusion. This risk has thrust cybersecurity into the forefront of available career opportunities. According to St. Louis Community College's State of St. Louis STEM Workforce Report, in 2013 there were over 23,000 STEM jobs available, but only 2,000 jobseekers looking for those opportunities. It is also predicted that there will be over 1 million jobs available by the year 2020 to protect our nation's cybersecurity infrastructure.

A critical part of our success to fulfill future needs is by engaging the youth of today to become interested in STEM. There are many great examples of cities taking initiative, and their success has been found on two fronts, curriculum adoption and competition engagement.

One of the important findings within our survey was the lack of trained personnel in cybersecurity. The educational standards for the state do not have any requirements for curriculum focused on computation. Currently the state is doing some level of participation in cybersecurity training. Several schools are currently participating in Project Lead the Way's Computer Science program with some degree of success. The adoption rate has been high, but schools are experiencing some challenges to implement.

- The cost may be prohibitive to some small and rural schools in the state.
- The ownership of the teaching becomes hard due to instructors with little knowledge or background on the subject.
- Many districts are categorizing cybersecurity curriculum into the business department.
- It doesn't align with the critical certifications employers are looking for when hiring.

The need for educators holding degrees in computing is not one of the areas of acceptance by American Board for Certification of Teacher Excellence (ABCTE). The closest one comes to a computation related field of study is that of tech and engineering in the traditional route. The pipeline of educators teaching computing is therefore limited in the state.

Recommendation: Modification of High School Curriculum

Currently there are no guidelines for cybersecurity related studies within the K-12 system. It is therefore our recommendation that the State of Missouri and the Department of Elementary and Secondary Education (DESE) modify the curriculum to add cybersecurity related studies in the K-12 framework as has been accomplished by few other cities and states. In concurrence with the previous recommendation for creating a cybersecurity institute, the state can provide resources to partners who will advocate for furthering curriculum adoption and partnering with interested schools. The institute can work closely with DESE to ensure a minimum viable product will be created in which all schools can easily incorporate courses into their curriculum. We would also recommend collaborating with the Cyber Texas Foundation to provide subject matter expertise to the state. Their support will expedite the process.

Recommendation: Cybersecurity studies specialization for teachers

The lack of trained personnel teaching cybersecurity studies is a major gap and this requirement needs to be met to support the changes to the K-12 curriculum to incorporate cybersecurity studies. Currently no such specialization exists in the teacher training programs and degrees and hence our recommendation is to create a standalone specialization in cybersecurity studies to the educational training program.

Gap #3: Importance of Internship Opportunities

Internships offer numerous benefits to both the student and the offering organization. The student obtains real world, hands-on experience within cybersecurity, and in many cases, the intern will go on to work within the offering organization. In regards to the survey responses, 34 of the 48 responses indicated that internships and internship opportunities are important in their industry. However, there are not enough internship opportunities available for the demand.

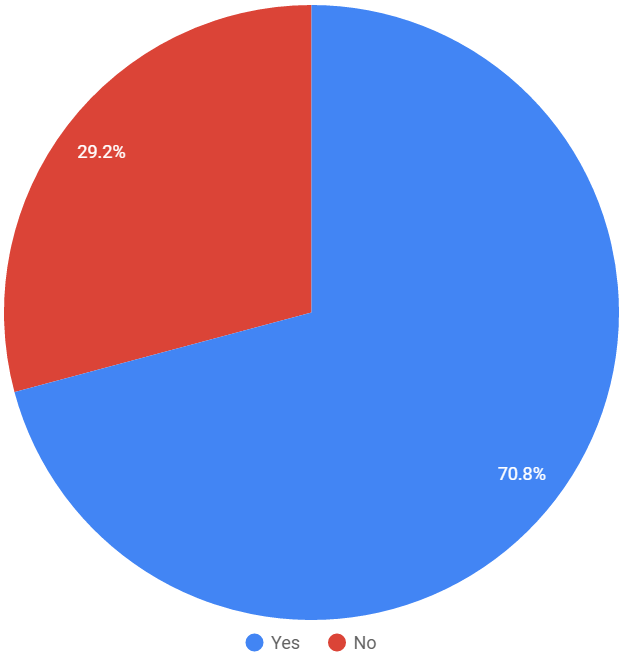

Figure 4: Survey participants' response to the importance of internships.

Recommendation: Centralized Internship Registry

The State of Missouri should provide a centrally coordinated registry to connect cybersecurity internship opportunities with potential interns.

Recommendation: Provide Private Sector Internship Incentives

The State of Missouri should provide the private sector with incentives that encourage them to provide more internship opportunities, which would also be included in the state's internship registry system.

Gap #4 Industry Certifications

Only 18 of the 48 responses indicated the importance of industry certifications. We feel this is an artificially low number considering the lack of private sector survey participants. Scanning daily job listings would indicate that the importance of industry-recognized certifications is much higher in reality.

Recommendation: Provide Certification Cost Reimbursements

The State of Missouri should provide cost reimbursements (in whole or partial) to those who obtain industry-recognized certifications in their field. This would encourage continued education, professional development, and adherence to the codes of ethics of the certification organizations.

Gap #5: Competitions and Student interest

Competitions provide students goals and necessary excitement which keeps them focused on a particular topic. Students typically spend time beyond classwork on the technical topics which foster learning that a typical coursework cannot provide. Competitions that require group interactions help students develop skills in group dynamics. Another outcome of such competitions is the technical writing that the student needs: from resume building to writing basic reports of incidents that they encountered during a competition. Within a curricular program, competitions have a symbiotic relationship that enables student to maintain interest and focus, allows faculty to interact with students as participants, and gives students the ability to hone their skills within a classroom environment. There are various competitions in which students at different levels can participate. Businesses understand the need of such competitions and they sponsor many of these initiatives. In addition, businesses recruit from the competitions.