Co-Op Light:

Developing a Cyber Security Workforce through Academia-Industry Partnerships

The need for cyber security professionals in the workforce will only continue to increase and the existing shortfall widen (Fourie et al., 2014). There are not enough people to fill the open positions. Yet, there are individuals with an educational background in cyber security that are not being hired. They do not have the required experience in many cases (Caldwell, 2013). Thus, we see organizations struggling to fill positions in cyber security, but unwilling to hire those without experience. Coincidentally, these individuals will never obtain the experience in cyber security if some employers do not take a chance on them.

Some programs have been able to address this problem directly, such as the NSF's Scholarship for Service (M. E. Locasto, Ghosh, Jajodia, & Stavrou, 2011). It provides students with an opportunity to work for a governmental organization performing cyber security work in exchange for a commitment by the student to work for the organization for a certain number of years. The program has been very successful. However, it is not an attractive option for every student since the service commitment may seem too long for some or the pay too low.

Internships have also been available for some, but generally are more difficult to find as employers are reluctant to hire individuals with little or no experience, even for internships. Some students may end up performing cyber security related work in a computer science or information technology internship, which may later be leveraged for a more cyber security focused position within the same or a different organization. Although for those seeking a cyber security internship in the first place, this is not necessarily an efficient or effective pathway.

Therefore, new approaches are needed for cyber security, including the increased use of older approaches that have proven track records in other disciplines. One approach that has been effective has involved partnerships between universities and industry. An example of this being done at a high and intricate level is Northeastern's Co-op program that requires students

to alternate between semesters of academic coursework with semesters of co-op experiences. This typically begins the second semester of their sophomore year. Although highly successful and a model of effective co-op education, it does require a significant amount of coordination, relationship building with industry partners, and an institutional willingness to transform the educational structure of a university. Northeastern has been doing it this way for years and it works for them (Smollins, 1999). For other universities without this history, there may be significant bureaucratic and institutional hurdles to develop a co-op model for just one or more programs. Likewise, it can take several years to develop the necessary relationships, both within the institution and with external partners.

An effective approach for many universities may try and combine elements of internship programs with those of a co-op model to provide a more holistic educational approach to cyber security workforce development (Hoffman, Burley, & Toregas, 2012). One could think of this as "co-op light." This approach has been employed at some universities (M. Locasto & Sinclair, 2009), as well as the University of Washington under the coordination of the Center for Information Assurance and Cybersecurity (CIAC). During the initial stages of the development of this program, the University of Washington has partnered with a large corporation that has its headquarters in the region. This corporation has significant needs for diverse cyber security talent, including both technical and non-technical positions available.

To garner interest with potential participants, various information sessions are held on campus, such as the University of Washington Bothell campus. Given the diverse nature of cyber security positions available with this corporation, it is often a matter of finding the right fit between a unit or division of the corporation and high-caliber students. In other words, students apply to participate in the program. Various hiring managers within the corporation that represent these diverse units or divisions then look through the applicants to see if there is a specific fit for their needs. This approach helps maximize the experience for both the student and the corporation.

CIAC provides a point of contact for all participants that serves as a professional career advisor to them. If issues should arise, this individual helps troubleshoot them on behalf of the

student. Additionally, a cohort model is employed that allows for shared experiences between students as they enter the various components of the program together. This provides a peer-support mechanism for these students that can be invaluable.

Part of this cohort model includes the completion of additional academic coursework together. This three-course sequence results in a cyber security-related certificate from the University of Washington's Professional and Continuing Education (PCE) component. It also satisfies the requirements of CNSS 4011, CNSS 4012, and CNSS 4016. Thus, students walk away from this program with an additional credential and valuable work experience. For most, this has resulted in job offers for the student from the corporate partner with most of these offers being accepted. This is a win-win for the student and corporate partner.

Thus far, this program is in the process of completing its second cohort with the third cohort on the way. Part of the design of this program involves feedback from stakeholders and participants on a regular basis so that improvements remain ongoing and continual.

Several lessons have been learned and are continually being adapted and applied. For example, the three-course sequence that results in a certificate from PCE was a pre-existing certificate program that was not designed with the unique needs of program participants in mind. One possibility for the future may involve designing a certificate program that is custom designed for these students. The original decision to use a preexisting certificate curriculum was made to optimize the use of existing resources and to minimize program overhead, especially when the success of the model remained uncertain. As the program continues to demonstrate a successful overall approach, the development of a tailor-made certificate curriculum should be revisited.

Additionally, the program currently has one corporate partner. New corporate partners are being explored to build upon these initial successes. Diversification and expansion of corporate partners will be vital to ensuring the continued success of the program and provide a broader number of industries students with an interest in cyber security can pursue.

This program does not replace other successful programs, such as Scholarship for Service or full co-op models (e.g., Northeastern). Nonetheless, it does help fill a void. It provides greater flexibility as is often seen in internships, but with increased structure, learning opportunities, and a cohort approach, as is often seen in co-op models. The overall risk in participating in the program, whether as a student or as a corporate partner is also quite low compared to other models that have been employed in the cyber security domain. There will never be a one-size-fits-all approach to address the significant shortage in the cyber security workforce. However, by continuing to be creative and willing to take chances, additional voids can be filled and successes recorded.

References

Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security*, *2013*(7), 5–10.

Fourie, L., Pang, S., Kingston, T., Hettema, H., Watters, P., & Sarrafzadeh, H. (2014). The global cyber security workforce: an ongoing human capital crisis. *Global Business and Technology Association*.

Hoffman, L., Burley, D., & Toregas, C. (2012). Holistically building the cybersecurity workforce. *IEEE Security & Privacy*, *10*(2), 33–39.

Locasto, M. E., Ghosh, A. K., Jajodia, S., & Stavrou, A. (2011). The ephemeral legion: producing an expert cyber-security work force from thin air. *Communications of the ACM*, *54*(1), 129–131.

Locasto, M., & Sinclair, S. (2009). An Experience Report on Undergraduate Cyber-Security Education and Outreach. In *Proceedings of the 2nd Annual Conference on Education in Information Security (ACEIS 2009), Ames, IA, USA*.

Smollins, J.-P. (1999). The making of the history: Ninety years of Northeastern co-op. *Northeastern University Magazine*, *24*(5), 19–25.