Co-Op Light: Developing a Cybersecurity Workforce through Academia-Industry Partnerships

Marc Dupuis
University of Washington Bothell
Box 358534
Bothell, WA 98011
marcjd@uw.edu

ABSTRACT

This paper presents a discussion on a cybersecurity co-op light model. Elements of an internship are combined with elements of a co-op to help provide students with an engaging work experience while also serving the needs of an organization.

CCS Concepts

• Security and privacy → Human and societal aspects of security and privacy • Social and professional topics → Professional topics → Computing education

Keywords

Co-Ops; internships; cybersecurity; workforce; partnerships.

1. INTRODUCTION

The need for cybersecurity professionals in the workforce will only continue to increase [1]. There are not enough people to fill the open positions. Yet, there are individuals with an educational background in cybersecurity that are not being hired. They do not have the required experience in many cases [2]. Thus, we see organizations struggling to fill positions in cybersecurity, but unwilling to hire those without experience.

2. BACKGROUND

Some programs have been able to address this problem directly, such as the NSF's Scholarship for Service [3]. The program has been 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 may also be an option for some.

Another 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.

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 [4]. 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.

3. APPROACH

An effective approach for many universities may involve combining elements of internship programs with those of a co-op model to provide a more holistic educational approach to cybersecurity workforce development. One could think of this as "co-op light." This approach has been employed at some universities [5], as well as the University of Washington (UW) under the coordination of the Center for Information Assurance and Cybersecurity (CIAC). During the initial stages of the development of this program, the UW partnered with a large corporation, T-Mobile, that has its headquarters in the region. Given the diverse nature of cybersecurity positions available within this corporation, it is often a matter of finding the right fit for a high-caliber student.

A cohort model is employed, which provides a peer-support mechanism for these students that can be invaluable. Part of this cohort model includes the completion of additional academic coursework. This three-course sequence results in a cybersecurity-related certificate. Thus, students walk away from this program with an additional credential and valuable work experience.

4. LESSONS LEARNED

Several lessons have been learned. For example, the three-course sequence that results in a certificate was a pre-existing certificate program that was not designed with the unique needs of program participants in mind. A custom designed certificate program may be more effective for students in the future.

This program does not replace other successful programs, but 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. There will never be a one-size-fits-all approach. However, by continuing to be creative and willing to take chances, additional voids can be filled.

5. REFERENCES

[1] L. Fourie, S. Pang, T. Kingston, H. Hettema, P. Watters, and H. Sarrafzadeh, "The global cyber security workforce: an ongoing human capital crisis," *Glob. Bus. Technol. Assoc.*, 2014.

[2] T. Caldwell, "Plugging the cyber-security skills gap," *Comput. Fraud Secur.*, vol. 2013, no. 7, pp. 5–10, 2013.

[3] M. E. Locasto, A. K. Ghosh, S. Jajodia, and A. Stavrou, "The ephemeral legion: producing an expert cyber-security work force from thin air," *Commun. ACM*, vol. 54, no. 1, pp. 129–131, 2011.

[4] J.-P. Smollins, "The making of the history: Ninety years of Northeastern co-op," *Northeast. Univ. Mag.*, vol. 24, no. 5, pp. 19–25, 1999.

[5] M. Locasto and S. Sinclair, "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*, 2009.

SIGITE '18, October 3–6, 2018, Fort Lauderdale, FL, USA
© 2018 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-5954-2/18/10.
https://doi.org/10.1145/3241815.3241880