# Suggestions for Addressing the Changing Needs of the Cyber Security Workforce

Dr. Char Sample, & Dr. Connie Justice

## Introduction

Cyber Security programs continue to expand across universities creating their own academic silos in response to growing workforce demands for cyber security professionals. Strong industry growth justifies this growth pattern in cyber security programs. These programs continue to turn out specialists that support the market demand.

However, a growing chorus have observed the need to break down silos, and are also calling for cross-disciplined approaches to solving cyber security problems (Peltsverger, 2015; Rowe, Lundt & Eckstrom, 2011; Crowley, 2003). Disciplines such as law, psychology, sociology, resilience, reliability, statistics, data science, international studies and others are becoming increasingly intertwined with cyber security (Ibid). The existent cyber security programs across accredited universities overwhelmingly continue to offer the same courses in penetration testing, policy, reverse engineering, risk, forensics, management and computer/network architecture; thus, Peltsverger's study of 2015 is still very applicable today.

In order to support the growing need for cross-discipline cyber security professionals, accredited cyber security programs will need to update their focus to not only embrace other academic disciplines, but also to understand how those disciplines can contribute to the improvement of cyber security and vice versa. A potential first step in this journey may begin with the offering of a security architecture course, where students are forced to acquire a cursory knowledge of other disciplines in creating a workable security solution.

Traditional architects combine knowledge from various disciplines in order to design structurally sound buildings (Savold, Dagher, Frazier, & McCallam, 2017). Similarly, security architects use skills learned in other disciplines to create robust network security solutions that support organizational goals. Creating strong defensive networks in support of a mission requires a mix of breadth and depth in the skill set of the network architect (Triolo, 2014).

## Background

Academia silos exist because expertise is gained through research that focuses on a specific discipline while excluding others. Studies are purposefully tightly

restrained to allow the researcher to focus on a specific problem. Variables are limited, so that results or findings can be generalized for application where the same variables appear in different environments. Thus, cyber security would naturally follow the same structural pattern. This ultimately leads to cyber security professionals who are unable to effectively communicate with other groups in the workplace.

Cyber security programs have responded to industry's demand for skillsets. This approach showed initial successes. However, like nursing where professionals initially took care of patient's immediate needs, programs evolved to include increasing numbers of courses and disciplines (psychology, chemistry, sociology, kinesiology, etc.) in order better prepare nurses for their jobs. So too, cybersecurity curricula must evolve to include other disciplines with the goal of improving the students for the future workplace.

Cyber security is increasingly being asked to support other disciplines (law, finance, psychology, sociology, etc.) yet the programs are not reflecting this in their curricula. This failure to adequately support other disciplines further isolates cyber security professionals and may limit the students to becoming industry commodities. Commodities are quickly picked up and discarded this can be problematic for career growth.

These factors increasingly suggest the need to restructure cyber security programs away from the silo approach and into the cross-disciplined approach. The overall problem facing educational institutions, and students is that accredited programs may not adequately prepare their students for cybersecurity workforce challenges where diverse skill sets are becoming increasingly important. The general problem is the universities are focusing on technical rather than the holistic education of the cybersecurity learner when the workforce has a growing need for the holistic cybersecurity professional (Triolo, 2014).

**Proposed Solutions**

There are several potential solutions to the cyber security silo problem and each one warrants discussion. The proposed solutions are not limited to those discussed here and are likely highly situational. In some cases, some institutions may find some programs unworkable, for this reason these are suggestions not requirements.

1. Create a liaison position in the departments that interacts with other disciplines. This approach would entail hiring a liaison who reaches out to different

departments and works to define the necessary courses to make cyber security a joint major with the available disciplines.

2. Embed departments together for work on a common goal. An example of this approach occurs at Cardiff University in Wales where criminal justice, cyber security, data science, psychology, computer science exist in teams that work together in solving common research problems.
3. Require cyber security to be a dual major or joint major at the undergraduate level. This would force cyber security students to understand how cyber supports other disciplines and communicate with personnel in a manner that demonstrates an understanding of the discipline..
4. Create distinct curriculum for cybersecurity majors that include, but not limited to; cybersecurity risk assessment, creating policies, third party risk, and network security architecture.
5. Create cybersecurity curriculum for all disciplines to take before taking curricula in specific disciplines. See figure 1. Additionally, we could create common cybersecurity curriculum before discipline specific curriculum and midway or end of discipline specific curriculum, see figure 2.

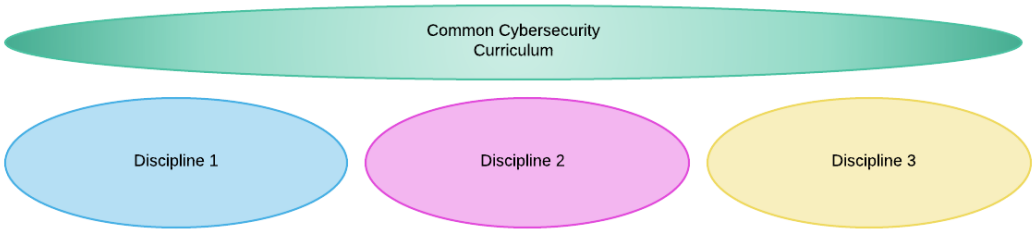


*Figure 1*: Common cybersecurity curriculum

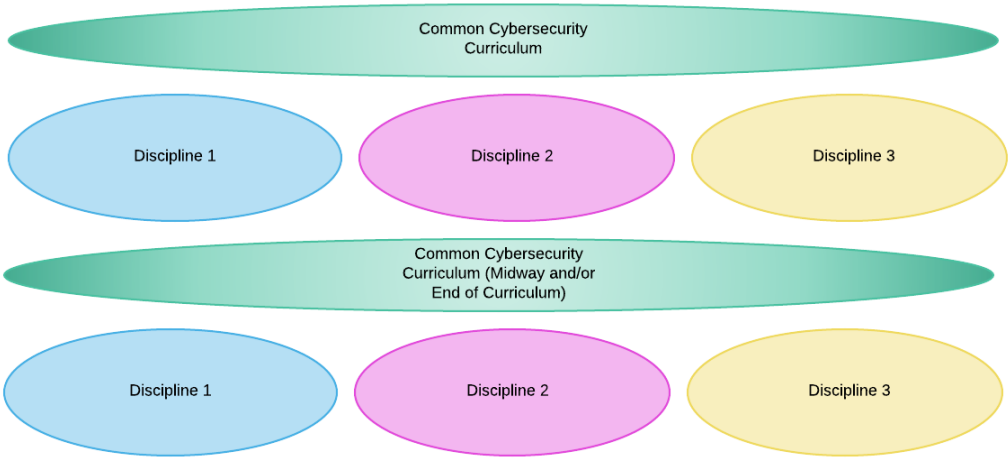


*Figure 2*: Common cybersecurity curriculum before and midway and/or end of curriculum

Specialized roles such as penetration testers and reverse software engineers provide an entry point into an organization, but generally speaking not professional growth opportunities Triolo (2014) noted that attackers need to be correct once and defenders need to be correct every time. A certain set of skills must bridge the gap between attacker skills and defender skills.

"Security architects design, build and oversees the implementation of network security for an organization" ("Become a security architect", n.d.). The security architect is entrusted to create a solution that reflects a deep technical knowledge of security products, and how to integrate those products in support of organizational goals. Solutions are complex and must work (Ibid). This mix of technical skills, management skills and people skills are unique. Introducing this mix of skills in cyber security programs as a foundational course would provide a foundation for a wider path of experiences for students and a potential bridge for those wishing to focus on policy.

Security professionals are frequently reminded to "bake in" security, not "bolt it on". This security by design must be engineered to the environment and processes that the security solution supports. Designing in security requires other disciplinary knowledge outside of the traditional technical areas.

Many universities and colleges participate in capture the flag cyber challenges that require participants to act as both attackers and defenders (Manson & Pike, 2014). These exercises are primarily focused on vulnerability exploitation, with prevention

being covered as a reaction to attack signatures (Manson & Pike, 2014). In some cases the cyber challenges require teams to build resilient solutions, but once again these solutions are designed to withstand known attacks in general. Creating and building of defences, in this arrangement, becomes an ad-hoc process that lacks rigor.

**Conclusion**

The changing nature of problems requiring cross-discipline approaches to cyber problems will force change in educational institutions programs. These changes will need to recognize the importance of other academic disciplines in creating the next generation of cyber security professionals. This paper put forth suggestions to offer potential ways forward.

**References**


Andel, T. R. and J. T. McDonald (2013). A Systems approach to cyber assurance education. *Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference.* Kennesaw GA, USA, ACM**:** 13-19.

Become a security architect. (n.d.). Cyber Degrees. Retrieved from https://www.cyberdegrees.org/jobs/security-architect/

Henry, A.P. (2017). "Mastering the cyber security skills crisis: realigning educational outcomes to industry requirements" ACCS discussion paper no. 4, August 2017, Australian Centre for Cyber Security, UNSW

Canberra, Canberra, viewed 26 Feb 2018, Available: https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/ACCS-Discussion-Paper-4-Web.pdf

Crowley, E. (2003, October). Information system security curricula development. In Proceedings of the 4th conference on Information technology curriculum (pp. 249-255). ACM.

Joint Task Force on Cybersecurity Education (2017). Cybersecurity Curricula 2017. Available: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Knapp, K. J., et al. (2017). "Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance." Journal of Information Systems Education 28(2): 101-113.

LeClair, J., et al. (2013). An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce. Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference, ACM, (LOCATION).

Peltsverger, S (2015) "A survey of university system of Georgia cyber security programs" , Proceedings o the 2015 Information Security Curriculum,

Manson, D. and R. Pike (2014). "The case for depth in cybersecurity education." ACM Inroads **5**(1): 47-52.

McGettrick, A., et al. (2014). Toward curricular guidelines for cybersecurity. *Proceedings of the 45th ACM technical symposium on Computer science education*. Atlanta, Georgia, USA, ACM**:** 81-82.

Murphy, D. R. and R. H. Murphy (2013). Teaching cybersecurity: Protecting the business environment. *Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference*. Kennesaw GA, USA, ACM**:** 88-93.

NISTIR 8193 (DRAFT), National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators: Indicators for Performing Work Roles. (n.d.). Available: https://csrc.nist.gov/publications/detail/nistir/8193/draft

Ramirez, R. B. (2017). Making cyber security interdisciplinary: recommendations for a novel curriculum and terminology harmonization, Massachusetts Institute of Technology.

Savold, R., Dagher, N., Frazier, P., & McCallam, D. (2017, June). Architecting Cyber Defense: A Survey of the Leading Cyber Reference Architectures and Frameworks. In *Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference* on (pp. 127-138). IEEE.

Triolo citation - https://www.scmagazine.com/hackers-only-need-to-get-it-right-once-we-need-to-get-it-right-every-time/article/537904/

**Dr. Connie Justice**
Department of Computer Information and Graphics Technology
Purdue School of Engineering and Technology
Indiana University Purdue University Indianapolis
cjustice@iupui.edu
317.278.3830

Dr. Connie Justice has over 30 years' experience in the computer and systems engineering field. Professor Justice is a Certified Information Systems Security Professional, CISSP. She created the networking and security options for CIT majors and a Network Security Certificate Program. She has designed and modified many courses in networking and networking security curriculum. Professor Justice is noted for her creation of the Living Lab, an experiential learning environment where students gain real world experience running an IT business.

Professor Justice takes extreme pride and is a great innovator in the area of experiential learning and service. Professor Justice has published several papers on creating course curriculum for information assurance and security. Professor Justice enjoys connecting students with industry projects that can provide them much needed hands-on experience.

Dr. Justice consults for and has managed IT departments in small, medium, and large sized businesses. She serves as Senior Security Advisor for a fortune 100 company. Her areas of research include: experiential and service learning, information and security risk assessment, risk management, digital forensics, network security, network and systems engineering, network and systems administration, and networking and security course development.

Dr. Char Sample

Dr. Char Sample is research fellow employed for ICF International at the US Army Research Laboratory in Adelphi, Maryland, and is also with the University of Warwick, Coventry, UK. Dr. Sample has over 20 years experience in the information security industry. Most recently Dr. Sample has been advancing the research into the role of national culture in cyber security events. Presently Dr. Sample is continuing research on modeling cyber behaviors by culture, other areas of research are information weaponization, data fidelity, and deceptive data.