An Analysis of Academic Background Factors and Performance in Cyber Defense Competitions

Jim Hoag
Department of Information Assurance and Technology
Champlain College
Burlington, Vt. 05401, USA
jhoag@champlain.edu

ABSTRACT: *As Cybersecurity evolves as a field, academic programs in higher education respond to include new content and activities. To prepare the next generation of Cybersecurity professionals, curriculum are modified, new courses developed, and cybersecurity-based extra-curricular activities are increasing in popularity. Collegiate Cyber Defense competitions have emerged to give students an opportunity to experience real-life situations and have also received attention as a learning environment. This study examines the curriculum and other factors at schools participating in National Collegiate Cyber Defense Competitions to analyze institutional factors that might be associated with performance in the competition. The results indicate that there is no obvious connection between team academic characteristics and the outcome of the competition*[1].

Keywords: Cyber Defense Competition, Security Education

Received: 10 January 2015, Revised 9 February 2015, Accepted 17 February 2015

1. Introduction

Cybersecurity is a field that is evolving rapidly and becoming significantly more important in government and industry processes as well as technology education. Many colleges have implemented some form of Cybersecurity (Information Assurance, Information Security) curriculum. The number, breadth, and depth of courses are evolving to respond to the growth of the field.

[1] The abstract from this paper was presented in a roundtable discussion at the 2014 Colloquium for Information Security Education (CISSE) in San Diego.

At one time, it may have been sufficient to have a single course in Computer Security. This has changed as the field has grown and currently multiple courses are required for a comprehensive curriculum that addresses the major components of Cybersecurity. As the security landscape changes and threat models evolve, colleges re-factor the role of security course content that needs to be modified or added to academic programs

The field of Cybersecurity integrates concepts and skills from a variety of areas including Computer Science, Cryptography, Information Systems, Databases, Networks, Digital Forensics, and Information Security Project Management. The inter disciplinary nature of the field also includes business process, management, policy, law, and criminal justice. The curriculum for security has emerged in various academic departments: Computer Science, Information Technology, Criminal Justice, and Business. In some cases, new majors specifically targeting this area have been developed, some focusing on management and policy, while others emphasize technical skills and knowledge. In the latter case, curriculum and the associated lab activities need to facilitate students' development of a combination of skills and knowledge to meet the professional needs in these areas. There is significant interest from government and industry in encouraging growth in education programs in this area. The designation of colleges as Centers of Academic Excellence in Information Assurance was developed to promote programs that provide an effective foundation for this field.

Due to the nature of this field, a number of collaborative security events, activities, and competitions have emerged, developed by early adopters and enthusiasts. There has been the development of a variety of competitions that give opportunities to assess and enhance skills. The competitions include skills assessments; capture the flag events, and Cyber Defense competitions. The latter has become a formalized system in higher education with the Collegiate Cyber Defense Competition (CCDC). This event mimics real-life issues managing and defending an enterprise network. These events have gained popularity as students enjoy the challenge and learn a great deal.

Performance in the competition and qualifier events should be associated with the team's preparation for the event, which presumably would include courses in the curriculum at their institution. This may be increasingly relevant as programs might begin to include learning and environmental elements of the CCDC.

As both the competition events and academic efforts have evolved, there are components of security education involved, with possible common topics. There have been efforts to determine the impact of Cyber Defense competitions on curriculum and programs [1, 9, 10]. It seems there would be benefits from analyzing the effect of curriculum and academic programs on performance in competitions. Thus, the following questions have been developed to investigate factors in the team backgrounds.

Research Questions

- Does certification of an institution as a Center of Academic Excellence in Information Assurance suggest that a team would have an academic background that would help prepare them for success in CCDC?
- Is there a base program or set of courses that give students a firm foundation for the CCDC?
- Does the number of specific security courses required or available in a major provide a foundation for success in Cyber Defense competition?
- Do the majors and makeup of the team have an effect on performance in the competition?

2. Background

To investigate factors that may be associated with performance in Cyber Defense Competitions, it is necessary to provide background on cybersecurity curriculum, the competitions, and the impact and potential relationship between them. This section will give an overview of Cybersecurity curriculum, background and description of the Cyber Defense Competitions, and the impact of competitions on curriculum. In addition, the classification as Center of Academic Excellence in Information Security may be significant.

2.1 Information Security Academic Programs

Information Assurance and Cybersecurity academic programs are a fairly recent field in higher education, with most being less than ten years old. Although this is a new academic area, there are guidelines and suggestions for Information Assurance programs [6, 7, 10, 12, 20]. There are also a number of government and industry standards that can be and are used as a basis for curriculum [18,19] and suggestions for curriculum [1, 5, 20].

A normal evolution for Cybersecurity curriculum in many cases has been to add security course/content to an existing major. The addition may be a senior-level course with security concepts and skills building on top of the core major curriculum. If more than one course is developed, there might be a series of courses designed to be a concentration area or focus. Some institutions have developed majors targeting this field. As the content of the field expands, it becomes increasingly more difficult to cover all areas. A college needs to determine the scope of the major, as it is difficult to offer a comprehensive Cybersecurity background in an undergraduate program.

The makeup of the curriculum varies between institutions. Policy-managerial curriculum can be combined with a variety of majors and lend themselves to lecture and project management components. Technical curriculum would incorporate a heavy hands-on component. In technical courses, it has been clearly established that hands-on activities and active learning help increase effectiveness [1,4,12]. Academic programs give varying degrees of exposure or experience with cybersecurity knowledge,tools and skills. There are also many graduate programs based on Information Assurance/Cybersecurity. The focus of this investigation is traditional undergraduate curriculum as the makeup of the cyber defense teams is primarily undergraduate students.

One benchmark for a curriculum in information assurance is certification as a Center of Academic Excellence in Information Assurance/Cyber Defense (CAE/IA/CD). The goal of the designation as a CAE/IA/CD is: "*to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA and producing a growing number of professionals with IA expertise in various discipline*" [6]. This designation at that time indicated a school has a curriculum matching the standards of National Security Telecommunications and Information Systems Security (NSTISSI) 4011 and 4013 and provides outreach services, involvement in security activities, and that faculty strives to stay current and contribute to the field. The designation criteria was revised in 2013 replacing the standards with Knowledge Units [6].

2.2 History of CCDC

The Collegiate Cyber Defense Competition (CCDC) was initiated in 2004 as a result of efforts of educators, students, government and industry representatives gathered discussing the feasibility and desirability of cyber security exercises with a uniform structure for post-secondary level students [16].

The CCDC focuses on the operational component of a network administration, including administrative duties, management issues, policy for an existing information system. Scores are based on detection and response to external threats, availability of services, response to business requests and balance security needs against business needs [16]

The CCDC mission statement provides a summary of the motivation and goals for the competitions:

> *To provide institutions with an information assurance or computer security curriculum a controlled, competitive environment to assess their student's depth of understanding and operational competency in managing the challenges inherent in protecting a corporate network infrastructure and business information systems.*

CCDC Events are designed to:

- Build a meaningful mechanism by which institutions of higher education may evaluate their programs.
- Provide an educational venue in which students are able to apply the theory and practical skills they have learned in their course work
- Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams
- Create interest and awareness among participating institutions and students.

A description of the competition and overview is provided by the National Cyber Defense Competition [6]:

> CCDC competitions ask student teams to assume administrative and protective duties for an existing 'commercial' network – typically a small company with 50+ users, 7 to 10 servers, and common Internet services such as a web server, mail server, and e-commerce site. Each team begins the competition with an identical set of hardware and software and is scored on their ability to detect and respond to outside threats, maintain availability of existing services

> such as mail servers and web servers, respond to business requests such as the addition or removal of additional services, and balance security needs against business needs. Throughout the competition an automated scoring engine is used to verify the functionality and availability of each team's services on a periodic basis and traffic generators continuously feed simulated user traffic into the competition network. A volunteer red team provides the 'external threat' all Internet-based services face and allows the teams to match their defensive skills against live opponents.

Competition Overview

The CCDC is a three day event and the first competition that specifically focuses on the operational aspect of managing and protecting an existing "commercial" network infrastructure. Not only do students get a chance to test their knowledge in an operational environment, they will also get a chance to network with industry professionals who are always on the lookout for up and coming engineers. CCDC provides a unique opportunity for students and industry professionals to interact and discussmany of the security and operational challenges the students will soon face as they enter the job market.

CCDC not only benefits the students involved, but will also benefit corporations as these graduates will be bringing a more experienced skill set to their jobs upon beginning their employment. CCDC also provides direct feedback for schools to exercise, reinforce, and examine their security and information technology curriculum [6].

2.3 Relationship of Student Learning, Curriculum, & CCDC

While the CCDC has merit as an event to assess student's skills, faculty have also noted the learning opportunities and educational benefits[1,2,3,9,11].The hands-on, real-time, comprehensive nature of the activities provide enhanced learning and motivation as well as effective methods for teaching and learning security and administration skills. Adding topics to the competition such as management injects, policy, help desk, and incident reports gives experience in broad areas of infrastructure protection in an enterprise.

The experience augments and enhances learning concepts and skills taught in more traditional courses. The learning approach is effective enough that there has been impact on curriculum [1, 11, 15]. Schools are trying to integrate components of the experience into courses and adapt the three- day experience into a full-term course [4, 14]. This is an opportunity to learn how to solve large complex problems as a group. The comprehensive nature and pressure also provides opportunities to manage, prioritize, collaborate, and communicate. Student planning and practice prior to events and reflection after competitions are additional elements of the learning experience. Many feel that effective security curriculums should include hands-on activities throughout the curriculum to develop security concepts [1, 4, 12].

In some cases, a semester-long capstone course has been developed based on the components of the competition [14, 4]. Some schools use an ongoing red-blue competition [14] while others have a class that is used for training for the competition [11].

Certainly to secure applications, one must be aware of coding practices and computer theory. A knowledge of operating systems (theory and applied) and systems administration is necessary to harden systems and respond to incidents. Defense-in-depth requires understanding all critical components of a modern information system and how to secure them. As the field grows, this may be beyond the capability of a single undergraduate curriculum and academic programs might become more focused on particular areas. The competition results, team reflections, and feedback from judges provide information to schools regarding their approach to education in this field. Some components of the learning environment of the cyber defense competitions may be integrated into security courses.

2.4 Preparation for Career

Many connected with Cyber Defense competitions feel that these events are a good method of providing experience, knowledge, and skills that prepare a student for a career in Cybersecurity[8, 9, 13, 16]. Similarly, academic programs are designed to lay a foundation for careers in this field. As the need for professionals in this field grows it will be only natural to try to identify the critical skills and knowledge. The National Initiative in Cybersecurity Education [17] Workforce Framework is one such effort where knowledge, skills, and abilities associated with categories of cybersecurity professional functions.

The goal of many technical academic programs is to provide a foundation for careers in the field. A standard academic program will do this through courses based on computing, networking, and security components. The competition does this in a comprehensive environment with real-time, real-life scenarios. Professional certifications are another method of establishing competency in a field. A number of certifications exist for cybersecurity. However, few of them apply to college students and would not likely be a factor in team background.

3. Analysis of the 2012-2014 National Collegiate Cyber Defense Competition

An analysis of factors that might affect performance in schools participating in the National CCDC might help determine academic elements that provide a foundation for this type of activity and learning. The NCCDC competition involves ten teams from the United States regions. For the analysis described, the finalists that competed in the National Collegiate Cyber Defense Competition (NCCDC) in 2012,2013, 2014 were used for comparison. These teams won their respective regional competitions and were thus successful in competitions involving 8-15 colleges prior to competing in the national event.. Many of the regional finalists make it to the national competition in multiple years. Thus a total of nineteen different academic institutions competed between 2012 and 2014 and were used in the analysis.

Characteristics of these finalists might give an idea of backgrounds and factors that lead to effective performance. The factors analyzed include: certification as a Center of Academic Excellence in Information Assurance (CAE/IA), curriculum, number of security courses, class level, and majors of participants.

3.1 Methodology

Data was collected for each institution and entered into a table. A sample of the data is shown in Appendix A and the full dataset is available at https://sites.google.com/a/champlain.edu/jhoag or by contacting the author. Fields in the table included college website URL, Information Assurance related undergraduate majors offered, CAE/IA designation, course numbers for standard Computer Science (CS) or Information Systems (IS) degree requirements, and course numbers for common Information Assurance courses. This data was obtained from the college websites and catalogs. The types of degrees the school offered in relation to security were researched. A number of institutions offered a CS degree. Others offered a degree program more aligned with Information Systems. A few colleges offered both types of programs while a couple offered a program that was considered hybrid.

A CCDC team from a college where the relevant major is Computer Science might have a team comprised completely of Computer Science majors. However, some schools had multiple programs that might be associated with Cybersecurity and there are teams comprised of students from various academic programs. To gain a perspective on the academic background of the students, the majors and class-levels of the student teams were recorded where possible. This data was gathered from public information: the school's website, CCDC news announcements, or professional networking sites (i.e.Linkedin.com). CCDC rules allow for up to two graduate students on a team. The number of graduate students was noted when possible.

3.2 Results

The results relating to the first three research questions are summarized in Table 1. Colleges are ordered by the years they participated in the competition. This ordering might hopefully help determine any trends that might exist over time. The data can be associated with the research questions.

The first question asked if certification of an institution as a CAE suggests that a team would have an academic background that would help prepare them for success in CCDC. It was expected that teams doing well in the competitions came from schools with a CAE designation. Twelve out of the nineteen institutions were Centers of Academic Excellence in Information Assurance as indicated in the summary in Table 1. The results indicate that while a majority of the finalist teams come from schools designated as Centers of Academic Excellence, it is not a necessary indicator of success.

Research question two was related to curriculum and sought to determine if there is a base program or set of courses that give students a firm foundation for the CCDC. The academic programs and curriculum for the nineteen teams participating in the 2012-14 national competition were analyzed to determine whether a college offered a Computer Science program, Information Systems program, both, or a hybrid. The specific courses were used to evaluate the academic background of the team. The analysis included which standard CS courses were integral to the major, as well as the security, networking, and forensics. The required courses in the major were used and if a specialization exists for security, the required courses for the specialization were included. While schools had a number of electives, some relating to security, it would be difficult to determine how many of the students on the team had taken them.

College	CAE Y/N	Acad. Program CS/IS	No. of Security courses	Years in NCCDC 20XX
Univ. North Carolina	Y	CS	1	12
St.CloudUniv	Y	Both	IS - 6	12
Univ of Wyoming	N	CS	1	12
Texas A&MUniv	Y	CS	1	12
Univ. Washington	Y	CS	1	12,13
Cal Poly Pomona	Y	Hybrid	6	12,13
Millersville Univ.	N	CS	1	13
Rose-Hulman Institute	N	CS	1	13
Oklahoma State Univ	Y	IS	4	13
Dakota State Univ.	Y	IS	8	13,14
Univ. Central Florida	N	CS	1	13,14
Univ. Cal. Berkeley	N	CS	1	14
Southern Methodist U	Y	CS	5	14
W. WashingtonUniv	N	CS	2	14
North KentuckyUniv	N	Both	3	14
TowsonUniv	Y	Both	5	12,14
Rochester Inst of Tech	Y	Hybrid	5	12,13,14
Air Force Academy	Y	CS	3	12,13,14
UnivAlaska Fairbanks	Y	CS	3	12,13,14
Summary	**Y-12**	**CS 12**	**1**	**8 schools**
	N-7	**Both 3**	**2-4**	**5 schools**
		IS 2	**5-6**	**6schools**
		Hybrid 2	**>=7**	**1 school**

Table 1. Summary of Results

Based on the curriculum, students/teams were considered to have a primary background in Computer Science (CS), Information Systems(IS) background, both, or hybrid. A CS-based curriculum would include the traditional programming sequence, data structures and algorithms, calculus, theory courses with perhaps some networking/security courses. IS-based curriculums included programming, but also included components for systems administration, networking, and security. Both curriculums would likely have a database and operating systems course. Of the nineteen teams in the National finals in 2012-14, twelve had a Computer Science background, two had an Information Systems background, two were hybrid, and three schools had both CS and IS.

The third research question regarded whether the number of security courses was a factor in performance. The number of specific security courses associated with the primary major of the teams was estimated from the curriculum as presented in the college catalog. This is certainly a matter of interpretation and there may be security components to more standard courses or security courses offered as electives. However, the number associated with the major seemed a way to gauge the amount of exposure students might have had to Cybersecurity topics in coursework. One would assume that those schools making it to the finals would have a large number of security courses. The number of security specific courses ranged from 1-8 with one college having more eight courses. Five schools had 2-4 courses and, six schools had 5-6 security courses. However, the fact that eight of the schools had a single security course would seem to indicate that the number security courses is not a deciding factor.

To investigate the fourth research question regarding team composition the majors and class of the team members was researched. Most teams were comprised of a combination of third and fourth year students. Only a couple teams had graduate students as team members, The majors of the students were by and large the primary computer-security major of the institution. There were some students from related majors: Software Engineering, Computer Engineering. Teams from schools with both IS and CS majors were made up of members from each major. Those coming from schools with hybrid programs would have had courses from both areas. There does not seem to be any advantage based on team major and class composition.

The data was sorted by year of competition to indicate any apparent trends over time in the factors analyzed. The number of schools with CAE designation dropped from nine in 2012 to seven in 2013 to six in 2014. This may simply reflect that more schools that are not CAEs are participating in the competitions. The data in the table seems to indicated a clumping of schools with both IS and CS curriculum and Hybrid curriculum in 2014. However, further analysis indicates that each year, there were 6 schools whose curriculum was classified as CS-based and 4 schools that comprised the other three categories. There also was no clear trend in number of security courses associated with the major. Colleges that won all three years did have multiple security courses.

4. Discussion

The results indicate that within the factors analyzed, there are no clear-cut common background characteristics of the teams that would indicate a potential for success. While a majority of the teams came from schools designated as Centers of Academic excellence in Information Assurance, it is not a determining criteria for success in CCDC. Having courses in systems administration might be helpful but this is not a deciding factor for success, as only about one-quarter of the programs had a course in this area. An academic background with a number of security focused courses did not prove to be necessary or beneficial for a high level of performance in the competition. The majors and background of the team do not seem to impact success.

Thus, it is the team's preparative efforts that may be the major factor that contributes towards their success. In most cases, students start practicing in fall based on the previous year's competition and feedback. In addition, most schools have a pipeline of students from classes who can participate in concurrent years. A factor that emerged during the analysis is that winning one year is a good indicator of success in the ensuing years. Eight out of the 19 teams had been in the final competition in previous years.This may indicate that the method of preparation can be repeated, despite team members changing as they graduate. It might also seem that the longer a team competes in regional competitions, the better chance it would have at winning. However, 2013 was only the second year of competition for Rose-Hulman Institute of Technology in the Midwest Region, yet they won that contest against teams that had competed for many years.

As some of the elements of competitions migrate into traditional courses, we might expect to see an increase in the preparation that traditional courses play in success. It is probably not likely that a curriculum would be designed with learning outcomes focused on performance in a competition. However, the positive learning and motivation factors the competition provides may be able to be incorporated into undergraduate learning environments.

There are factors which might also affect any analysis of the data. Curriculum change over time, new colleges become designated as Centers of Academic Excellence, and more colleges are participating in the Collegiate Cyber Defense competitions. As the data was gleaned from college catalogs and CCDC information, it is open to interpretation. The goal of this project was to determine on a broad scale if there were obvious associations between academic factors and success in the competitions.

5. Future Directions

A similar analysis on regional competitions may provide more information. Since this analysis was performed on the teams that reached the national competition, student effort beyond academic preparation may overwhelm other factors. For novice teams, academic preparation may be a more significant factor. Further examination of team academic make-up including graduate and non - traditional students on the team could give some indication if this contributes towards success. Analysis of elective courses taken bystudents and other security based activities might yield some useful information. Interviews/surveys of the teams might also give more insight into what factors contribute to success, particularly their approach to preparation and coaching or mentoring. Analyzing the size of the academic programs might provide some indication of success based on number of interested students. In addition, factors like team-cohesiveness, self-efficacy might provide information that can be related to performance in the competition

6. References

[1] Adams, W., Gravos, E., Lacey, T., Leblanc, S.P., (2009), Collective Views of the NSA/CSS Cyber Defense Exercise on Curricula and Learning Objectives, *In*: Proceedings 2nd Conf. *Cyber Security Experimentation and Test*, Usenix Assoc., 2009.

[2] Bei, Y., Kesterson, R., Gwinnup, K., Taylor, C. (2011). Cyber defense competition: a tale of two teams. *Journal of Computing Sciences in Colleges*. 27 [1] , October 2011, p 171-177

[3] Bishop, M., Irvine, C. (2011). Hacking Competitions and Their Untapped Potential for Security Education. *IEEE Computer and Reliability Societies*, May/June 2011.

[4] Conklin, A. (2006). Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course. Proceedings of the 39th Hawaii International Conference on Systems Science 2006.

[5] Conti, G., Hill, J, Lathrop, S., Alford, K., Ragsdale, D. (2003). A comprehensive undergraduate information assurance program, Security education and critical infrastructures, Kluwer Academic Publishers, Norwell, MA,

[6] Cooper, S., Nickell, C., Piotrowski, V., Oldfield, B., Abdallah, A., Bishop, M., Caelli, B., Dark, M., Hawthorne, E. K., Hoffman, L., Pérez, L., Pfleeger. C., Richard Raines, R., Schou. C. (2009). Toward a Framework for Information Assurance Education, ITiCSE_2009

[7] Cooper, S. , Nickell, C., Pérez, L., Oldfield, B., Brynielsson, J., GencerGökce, A., Hawthorne, E. K., Klee, K. J., Andrea Lawrence, A., Wetzel, S. (2010). Towards information assurance (IA) curricular guidelines, *In*: Proceedings of the 2010 ITiCSE working group reports, June 28-30, Ankara, Turkey

[8] DHS http://www.dhs.gov/blog/2012/04/27/national-collegiate-cyber-defense-competition-nccdcretrieved 6/15/2015

[9] Educational Value of Competition: How Cyber Defense Competition Prepares Students For Careers. Interview with Dan Likarish and Rick Cisneros. Bankinfosecurity.com interviews Jan 9 2013. http://www.bankinfosecurity.com/interviews/educational-value-competition-i-1712 retrieved 6/16/2014

[10] Endicott-Popovsky, B. E., Popovsky, V. M. (2014). **Application of pedagogical fundamentals for the holistic development of cybersecurity professionals.** ACM Inroads , 5 [1], March 2014, p 57-68

[11] Hoag, J., Tanko, Z. (2011) The Impact of Cyber Defense Competitions on Student Motivation, Engagement, and Curriculum at Champlain College, *In*: Proceedings of the 15th Colloquium for Information Systems Security Education (CISSE), Dearborn, Ohio,

[12] Manson, D., Curl, S., Torner, J. (2009). A Framework for Improving Information Assurance Education, Communications of the IIMA. 79, 9 [1].

[13] Manson, D., Pike, R., The case for depth in cybersecurity education, ACM Inroads , 5 [1], March 2014, p 47-52

[14] Mauer, B., Stackpole, W., Johnson, D. (2012). Developing Small Team-based Cyber Security Exercises. Accessed from http://scholarworks.rit.edu/other/301

[15] Mullins, B. E., Lacey,T. H., Mills, R. F., Trechter, J. E., Bass, S. D, (2007), How the Cyber Defense Exercise Shaped an Information-Assurance Curriculum. Security & Privacy, IEEE Sept/Oct 2007, 5 [5] p. 40-49

[16] National Cyber Defense Competitions http://www.nationalccdc.org/

[17] National Cybersecurity Workforce Framework. http://csrc.nist.gov/nice/framework/

[18] NSA CAE http://www.nsa.gov/ia/academic_outreach/

[19] Smith, T., Koohang, A., Behling, R. (2010). Formulating an Effective Cybersecurity Curriculum, International Association for

Computer Information Systems

[20] Whitman, M. E., Mattord, H. J. (2004). A Draft Model Curriculum for Programs of Study in Information Security and Assurance, *In*: Proceedings of the 8th Colloquium for Information Systems Security, West Point, NY June.

Appendix A: Sample Data from colleges with different curriculum and programs: both IS and CS, IS, hybrid IS/CS, CS

	College Programs	CS & IS	Hybrid	IS	CS
	UG Degrees	CS, CIT	CIS	Network & Security Admin	Computer Science
CS	**SEC focus**	CIT-yes	yes, IA	yes	no
	CAE	no	yes	yes	no
	CS0 Intro to CS	CIT 130	CIS 231		CSSE 120
	CS1 Progr I	INF 120	CIS 234		CSSE 220
	CS2 Progr II - Data Structures	CS - INF 260	CIS 304	CSC 250	CSSE 230
	Web programming		CIS 311	CIS 275, CIS 375	CSSE 481
	Prog Languages				CSSE 304
	OS	CSC 460			CSSE 332
	Database	INF 282	CIS 305	CIS 484	CSSE 333
	Architecture/Organization	CSC 362	CIS 315		CSSE 232
	Algorithms	CSC 364			
	Computability	CSC 385			
	SWE/SW Design	CSC 439, 440	CIS 466		
	Other	INF 286			
SEC	**SEC+**			CIS 245	
	Web Security			CSC434	
	Pen Testing			CSC 436	
	Network Security	CIT 484	CIS 467	CSC 438	
	SW Sec		CIS 491		
	Net script/programming	CIT 383		CIS 468	
	Perimeter				
	Management				
	incident response				
	Crypto				
	catchall security	CIT 480	CIS 471	CIS 328 OS,	CSSE 442
	Auditing		CIS 433		
	Other		ACC 405		

NET	**NET+**	CIT 247		CIS 383	
	Telecom		CIS 307	CIS 363	
	Protocols		CIS 347	CIS 466	
	Sysadmin	CIT 271,371	CIS 447	CIS 460, 462	
	Routers			CIS 387	
	Network Design	CIT 447	CIS 437	CIS 385	
	NET catchcall	CIT 470			CSSE 432
FOR	**FOR I**			CIS 388	
	FOR II		CIS 481		
Summary	**Type of program**	Both	**Hybrid**	**IT**	**CS**
	SEC courses	3	**6**	**8**	
	team CS-IT background	both	**Hybrid**	**IS and CN&S**	**CS,CE, GR**

Research Data can be seen at: https://sites.google.com/a/champlain.edu/jhoag/ or by contacting the author