8-15-2020

First Year Students' Experience in a Cyber World Course - An Evaluation

Frank Breitinger
University of New Haven, frank.breitinger@unil.ch

Ryan Tully-Doyle
University of New Haven, rtullydoyle@newhaven.edu

Kristen Przyborski
University of New Haven, kprzyborski@newhaven.edu

Lauren Beck
University of New Haven, lbeck@newhaven.edu

Ronald S. Harichandran
University of New Haven, rharichandran@newhaven.edu

Publisher Citation

Breitinger, F., Tully-Doyle, R., Przyborski, K. et al. First year students' experience in a Cyber World course – an evaluation. Educ Inf Technol (2020). https://doi.org/10.1007/s10639-020-10274-5

First Year Students' Experience in a Cyber World Course - An Evaluation

Frank Breitinger (Corresponding author)* and Ryan Tully-Doyle and Kristen Przyborski and Lauren Beck and Ronald S. Harichandran

University of New Haven, 300 Boston Post Rd, West Haven 06516, CT, United States

*New affiliation: Hilti Chair for Data and Application Security at University of Liechtenstein; Email: frank.breitinger@uni.li

F. Breitinger. [FBreitinger@newhaven.edu] was an Assistant Professor for Computer Science at the University of New Haven and Principal Investigator for the grant leading to the development of the Cyber World Common Course. Dr. Breitinger recently change positions an is now an Assistant Professor at the University of Liechtenstein. ORCID: 0000-0001-5261-4600

R. Tully-Doyle. [RTullyDoyle@newhaven.edu] is an Assistant Professor in the Department of Mathematics and Physics. His primary research areas are in functional analysis and operator theory. He also works in mathematical modeling and analysis. ORCID:0000-0001-8570-7141

K. Przyborski. [KPrzyborski@newhaven.edu] directs the Common Course at the University of New Haven. She obtained a doctorate in Marine Science from the University of South Florida St. Petersburg. The focus of her doctoral studies was on the the ecology of harmful algal blooms. The pedagogy of science, critical thinking, and scientific literacy are her primary research interests today.

L. Beck. [LBeck@newhaven.edu] holds positions at the University of New Haven as Lecturer in the English Department and as Assistant Director of the Common Course (a required first-year course in critical thinking). She earned a Ph.D. in Interdisciplinary Theatre and Drama from Northwestern University. Her primary research interests lie in the intersection of the fields of Theatre and Sound Studies in mobile audio works that she calls 'ototheatre.' More recently, Lauren has begun to study the impact of theatre studies on pedagogical practice in non-theatre courses.

R.S. Harichandran. [RHarichandran@newhaven.edu] is Dean of the Tagliatela College of Engineering and is co-PI of the grant entitled Development of the 'Cyber World' Common Course at the University of New Haven that facilitated the work reported in this paper. He has led several curricular initiatives in the college, including the development of students' technical communication skills and entrepreneurial mindset.

Acknowledgement(s)

The work reported in this paper was supported by a grant from the Davis Educational Foundation established by Stanton and Elisabeth Davis after Mr. Davis's retirement as chairman of Shaw's Supermarkets, Inc. We acknowledge the following faculty from the University of New Haven who participated in teaching the Cyber World Course: Ibrahim Baggili, Guy-Serge Emmanuel, Michael French, Glenn McGee, and Matthew Schmidt.

Funding

This work was supported by the Davis Educational Foundation. Any opinions, findings, and conclusions or recommendations expressed in this work are those of the authors and do not necessarily reflect the views of the Davis Educational Foundation.

Compliance with Ethical Standards

Ethical Approval. All procedures performed in studies involving human participants were in accordance with the ethical standards of the Human Research Ethics Committee (HREC) and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Informed consent. Informed consent was obtained from all individual participants included in the study.

Conflict of Interest. The authors declare that they have no conflict of interest.

ARTICLE TEMPLATE

First Year Students' Experience in a Cyber World Course - An Evaluation

ARTICLE HISTORY
Compiled September 9, 2020

ABSTRACT
Although cybersecurity is a major present concern, it is not a required subject in University. In response, we developed *Cyber World* which introduces students to eight highly important cybersecurity topics (primarily taught by none cybersecurity experts). We embedded it into our critical thinking Common Course (core curriculum) which is a team-taught first-year experience required for all students. Cyber World was first taught in Fall 2018 to a cohort of over 150 students from various majors at the University of New Haven. This article presents the evaluation of our Fall taught course. In detail, we compare the performance of Cyber World students to other Common Course sections that ran in parallel and conclude that despite the higher workload students performed equally well. Furthermore, we assess the students' development throughout the course with respect to their cybersecurity knowledge where our results indicate a significant gain of knowledge. Note, this article also presents the idea and topics of Cyber World; however a detailed explanation has been released previously.

KEYWORDS
First year experience; cybersecurity; Common Course; Experience Assessment; Outcome Evaluation

1. Introduction

Cybersecurity is a growing concern for everyone; businesses, governments, individuals and educational institutions (Ponemon Institute, 2018). Consequently, information security was rated as the top concern for three years in a row by IT professionals (Educause, 2018) which led to a discussion of embedding computer science courses into the core curriculum and be taught to all students (required) (Nager & Atkinson, 2016).

This has been an ongoing discussion, e.g., Haigh (1985) 'Planning for Computer Literacy' discusses what computer skills need by students to succeed in their personal lives and careers. Nowadays, especially with the change of our online behavior, there are arguments to include cyber literacy, safety, and security (Sobiesk, Blair, Conti, Lanham, & Taylor, 2015; Stiller & LeBlanc, 2006; Werner, 2005). These are natural discussions as cybersecurity impacts almost all careers (corporate, government, finance, healthcare, military, etc.) as well as each individual. As a result, non-major cybersecurity courses gain more and more popularity. For instance, Loyola University in Maryland[1] offers a 'Cyber Security and Digital Forensics' addressing the basics

[1] https://www.loyola.edu/academics/computer-science/degrees/non-majors

of cybersecurity. The University of Washington, Bothell offered a similar non-majors course consisting of a lab section and teaching technical skills, such as developing a back up strategy or installing security relevant software (e.g., Virus scanner) (Dupuis, 2017).

At the University of New Haven, we decided to introduce a course named *Cyber World* focusing on various cyber-related issues such as fake news, protecting your online identify or best practices for social media. In total, eight topics were lectured all relating to living in a Cyber World. All details about the course have been released in earlier work by (Przyborski, Breitinger, Beck, & Harichandran, 2019). There, we provide a more detailed overview of the topics, the course layout, how we embedded the topics and some preliminary results on faculty and students perceived the course. A summary is provided in in Sec. 3.

While many agree that everyone should have some understanding of cyber-related topics, there are several challenges when including cyber-related material into a first-year experience. First, the Common Course is an existing course where outcomes are not related to cyber and the course already has significant content. Adding more material may be too much for students and negatively impact their performance (i.e., impact original course outcomes). Second, the student body comes from many majors represented on campus, while the content is very STEM oriented.

This paper focuses on the evaluation of the course results from our initial run in Fall 2018. We analyze the impact of including cybersecurity knowledge into a version of the Common Course on students. Such an inclusion will be most useful if the content of the first-year experience and the cyber content interact with each other in a neutral or positive manner. Specifically, we look at the following research questions:

- R1 Did adding additional material impact student's performance? i.e., were course outcomes impacted?
- R2 Were students able to comprehend the cyber-related material? i.e., did they gain domain knowledge?

We show that in general students lack knowledge in terms of cyber-related topics. Additionally, we show that including a topic like Cyber World into our common course did not impact the course outcomes, but overall students improved their knowledge of cybersecurity and now think more critically about it. Note, by design this course includes students from all majors on campus and thus it was interesting to see that also non-STEM majors performed well.

The structure of this paper is as follows: Section 2 summarizes the related work and previous similar studies. Next, we provide an overview of the Common Course and Cyber World. The core of the paper are Sections 4 and 5 which assess the course outcomes and assess the student progress with respect to cybersecurity knowledge, respectively. In Section 6, we discuss limitations in our study. The last section discusses our findings and concludes the paper.

2. Background and Related Work

The 'freshman seminar' or 'first-year experience course' is a common feature at many universities. The idea in its modern form is credited to Thomas Jones, the president of the University of South Carolina, who wished to orient incoming students toward an institutional bond. In 1986, bolstered by the success of their University 101 course, the University of South Carolina instituted the National Resource Center for The

First-Year Experience and Students in Transition (National Resource Center, 2019). First-year courses began to be developed at universities to meet the needs of an increasingly diverse group of incoming college students (Upcraft, 1993). The goals of early orientation courses were to increase contact between students and faculty, to improve retention and grades, and to increase student participation in the campus community (Smith & Brackin, 1993).

Project-Based Learning as a core principle of a first-year experience course was implemented by Worcester Polytechnic Institute (WPI) in 2004 after their Commission on the First-Year Experience identified that students should be engaged in "current events, societal problems, and human needs" (Heinricher, 2019). As the authors' of Project-Based Learning in the first-year note, project-Based Learning provides experiences that allow students to practice skills that they will need throughout their college years, including database research, evidence-based argumentation, synthesis of sources, and academic writing, as well as the so-called 'soft' skills of collaboration, communication, leadership, and project management. The Common Course at the University of New Haven borrows heavily from the WPI model, using project-based learning as a mode to guide students toward the development of skills that will help them transition to college-level work. Our version of the course pays extra attention to information literacy skills. Information literacy has been identified as particularly important in the twenty-first century's 'global information society' because of the changes in the ways that knowledge is produced, distributed, discovered, and interpreted due to the internet and associated technologies (Johnston & Webber, 2003).

Some universities require students to take computer science courses as part of a core general education science curriculum (Nager & Atkinson, 2016). Some of these courses focus on highly technical skills, while others are aimed at educating students more generally on the use of computer hardware and software. Our course, and others like it, acknowledge a need for new college students to learn how computer and internet technologies changes the ways that information is gathered and how it must be evaluated. The focus of the Common Course on information literacy aligns in logical ways to the content of cybersecurity, specifically relating to the prevalence of misinformation in a cyber-connected world. Information specialists like librarians have suggested an urgent need for courses that promote understanding of information reliability, particularly on the internet where it is often difficult to determine an author's expertise (Edwards, 2018; Gibson & Jacobson, 2018). First-year lectures, as well as inquiry and project-based classes, are places that discuss this sort of learning goal. Consequently, a librarian has been brought in as a ninth expert in knowledge literacy in addition to the presentations offered by the eight faculty. This form of literacy has been explicitly linked to cyber literacy as we have demonstrated the ways in which authority and bias detection skills are important for healthy conduct in an online environment.

Although students are frequently online and may have a basic understanding of dangers and security risks, the majority does not know how act responsibly in many online situations and to protect themselves (Korovessis, Furnell, Papadaki, & Haskell-Dowland, 2017). For instance, research shows that the most basic of personal data protection like locking one's phone with a PIN is often neglected (Breitinger & Nickel, 2010). On the other hand, (Ricci, Breitinger, & Baggili, 2018) showed that parents are worried about their children online behavior. In Cyber World we addresses this broader need for students to have some basic understanding of cybersecurity.

Given that cybersecurity impacts many sectors (finance, corporate, government, military, health care, etc.), universities started offering cybersecurity courses with a special focus on non-majors. The style and content of these cybersecurity courses for

non-majors vary greatly (Dupuis, 2017). Some of the topics covered in these courses are similar to Cyber World: cryptography, networking, social engineering, privacy, phishing or ethics; others also include computer science fundamentals like: encoding of information, distributed computing, machine learning or Internet of Things (Das, Voorhees, Choi, & Landwehr, 2017). Some examples:

(1) Loyola University in Maryland offers a 'Cyber Security and Digital Forensics' course that discusses the fundamentals of cybersecurity measures;
(2) University of Washington, Bothell, provided non-majors with a cybersecurity course that included a lab component, teaching technical skills to students, such as installing preventive software, or stressed the importance of periodically backing up information in the cloud (Dupuis, 2017);
(3) A non-majors interdisciplinary course has been offered entitled 'Cybersecurity for Future Presidents' at Le Moyne College which is similar to the one at Loyola (Das et al., 2017).

While some of the cybersecurity courses for non-majors were described as interdisciplinary, Cyber World seems to be the only course that actively sought to include professors in the fields of humanities and life science. We thus follow literature where more interdisciplinary collaboration is suggested. Hendler, Shadbolt, Hall, Berners-Lee, and Weitzner (2008) agrees that understanding cybersecurity fully may require theories and lessons from various disciplines. Furthermore, humanistic and technical expertise will benefit students by bringing the topic into subjects other than STEM and will assist in navigating ethical concerns (Tavani, 2002).

The assessment methods employed in this paper are based on rubric evaluation of student work. Rubrics were used as a formative assessment on a sequence of reflective papers and on a project-design proposal. Use of rubrics is a demonstrated best practice for measuring course and program design (Reddy & Andrade, 2010). In writing based-courses, rubrics are typically descriptive rather than quantitative (Dawson, 2017). Descriptive rubrics yield quality information if the rubrics meet written for clarity and focus (Brookhart & Chen, 2015). In addition to providing instructor and designer information about course effectiveness and design, which allows teachers to react to student reception and performance, rubrics also provide clear explanations of evaluation to students, who can use this feedback to improve their work. While in the past, instructors have viewed rubrics as a way to provide consistent and fair grades, over the last decade a significant shift in the study and use of rubrics as a teaching tool (Ragupathi & Lee, 2020).

3. Overview of the Common Course

The Common Course is a mandatory first year class and serves as the only core critical thinking experience at our University. It helps students to succeed in college by providing academic research and information literacy skills

Each Common Course is framed around an interdisciplinary theme. Previous Common Course themes included Justice, Identity, Politics, Happiness, and Societal Impact of Climate Change. Throughout the semester students participate in active discussions, work on assignments, and have a group project related to the course theme.

Each cluster of sections has about 80 students and is taught by 4 faculty members from different colleges, all of whom have expertise in a specific discipline that can be used to examine the topic in question. Every week students have a

Whole Group session (WG) where all 80 students meet in a lecture hall and one of the instructors gives an interactive presentation in her/his area of expertise. All talks are related in some way to the course theme.

Small Group session (SG) which is a breakout session of 20 students together with their individual instructor (identical instructor throughout the semester) to reflect on WG topics and work on skills related to course outcomes.

In order to get more expertise into the WG presentations, we usually run two identical themes per semester. This allows us to have 'guest speakers,' i.e., we invite instructors from the second Common Course section to present on their topic. Additionally, other external presenters are invited such as a Librarian to present on student resources.

Cyber World theme. In Fall 2018, we introduced a new theme named *Cyber World* with the expectation that students would gain cyber-related knowledge. The course included the following eight topics; each reflected the instructor's expertise under the umbrella of Cyber World (topics are in order):

(1) Digitization, Artificial Intelligence & Command Control
(2) The Performance of Truth
(3) Cyber Forensic Science: Should there be a backdoor to encryption?
(4) Noone Knows Who You Are in the Cyber World, Not Even You: How the Internet changes your identity
(5) Ethics and Artificial Intelligence
(6) Who Owns the Digital You?
(7) Social Engineering and the Power of Graphic Design in an Online Environment
(8) Cybersecurity Principles: How can I protect myself against attacks?

While two of the instructors were familiar with cybersecurity, the other six faculty members learned about cybersecurity principles and issues alongside the students, which ensured that lectures were not too technical and were easy to comprehend for first-year students.

A more detailed description of the course, the content of the lectures and some roadblock are presented by Przyborski et al. (2019). This article also includes the results of a survey given to course faculty that focused on the following three questions: (1) How did students and faculty rate the quality of the educational experience; (2) What were the perceived successes; and (3) What needs to be improved, why, and how.

4. Assessment of the Course Outcomes

This section evaluates the performance of students with respect to the course outcomes. The two main objectives are to determine: (1) Did students meet the course outcomes despite having a more content heavy course theme; and (2) How did students of the Cyber World section compared to other common course sections?

4.1. Grade distribution among different Common Course sections

The Cyber World version of the Common Course contained the same learning outcomes and assignments as other sections of the Common Course run during the same

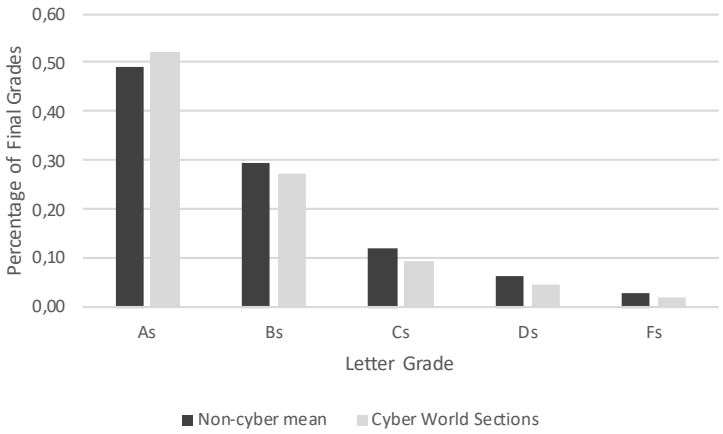


Figure 1. Grade distribution comparison for Cyber and Non-Cyber common course sections, F18. The following score ranges are associated with each grade: A 90-100; B 80-89; C 70-79; D 60-69; F < 60.

semester. However, because the Cyber World sections also required students to complete additional content related specifically to cybersecurity, course administrators were concerned that the grades of students in the Cyber World sections would be negatively affected due to the increased workload. To explore this topic, we analyzed the distribution of grades in each section of the Common Course compared to the grade distribution of the Cyber World sections. The course grades were normally distributed. Hence, we performed a two-tailed t-test against the null hypothesis that there would be no difference in grade distributions of the two groups.

Grade distribution results. A visual comparison of grades for all sections (see Fig. 1) indicated that there was likely little difference between the two groups. Table 1 shows the p-values for the two tailed t-test and confirms that the differences in mean grades between Cyber and Non-Cyber sections were not statistically significant at the 0.05 significance level. Hence, there is no evidence that the inclusion of cybersecurity topics had any effect on the grade distributions.

4.2. Specific assignment and rubric scores

Although there is clearly a connection between student attainment of learning outcomes and the grades they receive, studying section grades in isolation does not provide the entire story. Typically, grading criteria of individual instructors can include aspects of learning that are not measures of learning outcomes but are instead related to behaviors such as attendance and participation. Additionally, differences in grades of students can be due to differences in the way that instructors interpret rubric criteria.

The Common Course runs approximately 80 sections per year, necessitating the use of a large instructor pool. In an effort to maintain consistent grading across sections, common rubrics are used, and course faculty are trained in effective grading through the use of those rubrics. The pool of instructors teaching the course is somewhat stable, resulting in skilled faculty teaching the course who grade fairly consistently in comparison to each other. The Fall 2018 Cyber World faculty, however, had four instructors teaching the course for the first time who were not familiar with the grading methods and rubrics that have been developed for the course. During the ramp up to

Table 1. *t*-test comparison of differences in grade distributions between Cyber and Non-Cyber sections.

Grade	Section type	Mean % receiving grade	Variance	*p*
A	Cyber	.49	.05	.81
	Non-Cyber	.51	.05	
B	Cyber	.29	.03	.92
	Non-Cyber	.28	.04	
C	Cyber	.12	.01	.37
	Non-Cyber	.09	.00	
D	Cyber	.05	.00	.77
	Non-Cyber	.05	.00	
F	Cyber	.02	.00	.42
	Non-Cyber	.01	.00	

the Fall 2018 offering of the Cyber World Common Course, the demanding schedule of the full-time faculty teaching the course resulted in minimum time to participate in rubric and grading faculty development sessions.

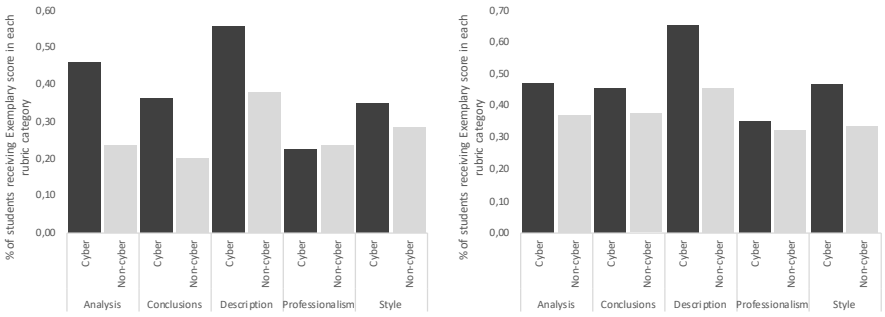
As part of the course assessment, course administrators evaluated the grading performances of the 'untrained' full-time faculty with those who had attended faculty development sessions. The evaluation of the effect of this training is important, because the additional work required of students in the Cyber World sections was greater than that of students who were in other sections. It was not clear if we would be able to separate the effect of faculty training from that of the increased workload.

Methods. There were two questions that we wished to address in terms of specific assignment grades. The first was a determination of the final scores of selected assignments, to see whether the overall grades received by students adequately accounted for grade criteria that fell outside of individual assignments. We also sought to determine what differences may have existed in rubric interpretation between Cyber and Non-Cyber faculty. The null hypothesis for both of these questions assumes that there was no difference in scores of individual assignments or in rubric interpretation between the Cyber and Non-Cyber topics. We focused on four assignments in order to simplify the analysis. These were the first and second academic reflection (AR1 and AR2), the final academic reflection (ARF), and the project proposal (PP). All of these assignments are important in terms of monitoring students' ability to demonstrate success in learning outcome attainment as they progress through the semester. Assignment scores were downloaded directly from the section gradebooks in Blackboard. Data were averaged for Cyber and Non-Cyber topics and the means were compared using *t*-test procedures.

Results. As shown in Table 2, AR2 and ARF showed no differences between groups, and the null hypothesis was accepted. For the AR1 and the project proposal (PP), significant differences were found between those students in Cyber sections and those in Non-Cyber sections. In both of those assignments, the scores were higher in Cyber

Table 2. Results of the t-test comparison for overall Academic Reflection 1 (AR1), Academic Reflection 2 (AR2), Final Academic Reflection (ARF), Project Proposal (PP). An * denotes those p scores that are significant at the 0.05 level ($\overline{x}$ = rubric mean).

Assignment	**Cyber**	**Non-Cyber**	p
AR1	$\overline{x} = 34.49$	$\overline{x} = 33.46$	.03*
AR2	$\overline{x} = 34.07$	$\overline{x} = 34.80$	.16
ARF	$\overline{x} = 108.1$	$\overline{x} = 108.7$	.57
PP	$\overline{x} = 82.18$	$\overline{x} = 69.26$	$< .0001$*



(a) Academic Reflection 1 (AR1). (b) Academic Reflection 2 (AR2).

Figure 2. Percentage of Cyber and Non-Cyber students receiving exemplary scores on Academic Reflection 1 (a) and Academic Reflection 2 (b) for five rubric categories.

sections than in Non-Cyber sections.

4.3. Rubric category differences

Common rubrics for assignments were used for all sections. In the case of the first two academic reflections the same rubric was used for both assignments. While differences between Cyber and Non-Cyber sections appear to be present (Fig. 2 (a,b)), it is difficult to discern how those differences changed within individual assignments and between each topic. The data for these rubrics were pared down by looking only at the percentage of students who received exemplary scores for each rubric category for the three assignments we considered.

Within the project proposal evaluation, the differences between the two groups of instructors is much more evident (Fig. 3). The categories that are typically seen in assignments across academic disciplines show the least differences between the two grading groups. This is most apparent in the "bibliography" and "organization" rubric categories. Other categories that are present for the project proposal assignment, but which might not be seen in typical academic courses within a specific discipline, reveal a more significant gap between the two groups. This can be seen especially in the way that the two groups of instructors graded the "Problem" portion of the assignment. Because students were randomly assigned to sections, it is unlikely that the students in the Cyber World sections were more skilled at creating a quality problem statement than the students in other topics. It is more likely that faculty untrained in the nuances of drafting a good problem statement did not recognize how students could improve

on the statements.

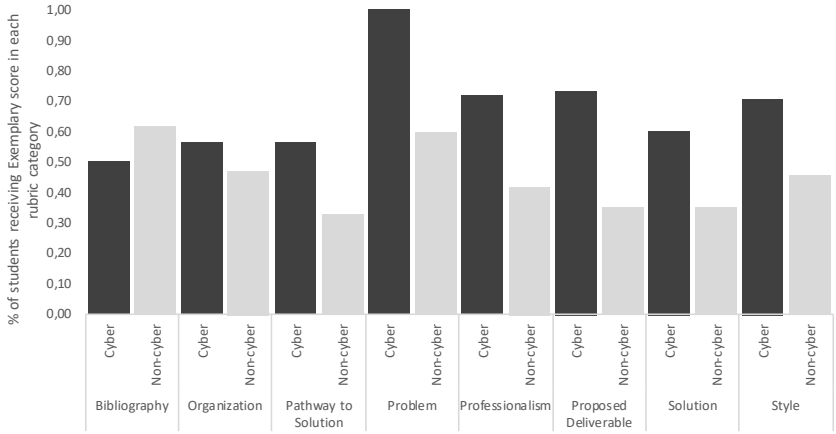


Figure 3. Percentage of Cyber and Non-Cyber students receiving exemplary scores on the Project Proposal (PP) for eight rubric categories.

Table 3. Rubric used to evaluate the three student reflections.

	Beginning - 1	**Developing - 2**	**Competent - 3**	**Accomplished - 4**
Use of cybersecurity terminology (C1)	Student does not utilize any terminology or frequently makes errors in usage	Student occasionally utilizes terminology with few errors	Student adequately uses terminology	Student consistently and accurately utilizes terminology
Concept understating (C2)	Student demonstrates no or poor understanding of cybersecurity concepts	Student demonstrates inadequate understanding of cybersecurity concepts (Student lists concepts related to cybersecurity)	Student usually demonstrates understanding of cybersecurity concepts (Student summarizes concepts related to cybersecurity)	Student shows understanding of key cybersecurity concepts (Student discusses in-depth/explains in detail concepts related to cybersecurity)
Application to real world (C3)	Student makes no practical application of cybersecurity	Student occasionally relates to real life skills	Student usually finds practical application to real life skills	Student is able to apply learning
Expresses personal concerns about technological issues (online identity, passwords, self-driving cars, AI, etc.) (C4)	Student does not indicate or indicates not having personal concerns about technological issues	Student indicates having concerns (1 sentence or brief list)	Student summarizes concerns (2-3 sentences, answer is more comprehensive)	Student is proactive, reacts to concerns (Installs application, changes privacy settings)

5. Assessment of Cyber World Material

In addition to the cross comparison with other Common Course sections (see Sec. 4), in the following we present the relative progress/achievement of students with regards

to cybersecurity-specific knowledge.

5.1. Methods

To garner an understanding of students' potential growth throughout the course, and to determine if they developed a more comprehensive knowledge of cybersecurity, the rubric in Table 3 was developed and implemented to score a series of three self-reflective essays written by students. Note, to evaluate the students during the course and to allow a comparison with other sections, Table A1 in the Appendix was utilized.

In order to create our rubric, we first researched the various types of rubrics used to assess student work (Allen, 2014; Karkehabadi, 2013; Office of Insttitutional Research and Assessment at the University of North Carolina, 2017) and ultimately decided on an analytic rubric because analytic rubrics provide a mechanism for the scoring of different behavioral elements or skills relating to cybersecurity knowledge. This allowed us to conduct a more in-depth analysis of students' overall comprehension. Additionally, the rubric includes a description of expectations for each score level, thus providing a level of consistency in scoring.

The elements to be scored were selected based on what the researchers believed to be important components of cybersecurity knowledge. These elements were:

Use of cybersecurity terminology measured if and how often students utilized cybersecurity-related terminology, and if it was used correctly. Definitions were guided by the US-CERT glossary[2] of cybersecurity terminology. Some terms, such as 'hacker' or 'hacking' that have entered the daily lexicon, were excluded from consideration.

Concept understanding refers to the ability of students to grasp cybersecurity concepts discussed throughout the course. This includes being able to accurately describe and explain ideas, theories, issues, and solutions. This was considered a relevant component as it is believed by the authors that concept understanding contributes to the proper use of terminology, application to the real world, and development of one's own ideas.

Application to the real world measured if students were able to utilize what they learned about cybersecurity through classroom lectures, readings, assignments, and group work. In other words, were they able to apply concepts to their everyday life and implement cybersecurity tactics to remain safe?

Expresses personal concerns about technological issues was utilized to see if the perspective of a student changed over the duration of the course. When reading the essays, we were also looking for proactive statements, i.e., did the student change some behavior, did s/he change privacy settings, or did s/he install applications (e.g., password manager).

In addition to the rubric, there were three questions that we tried to answer based on the content of each of the selected student reflections:

Q1 Are you worried about your online identity? - This question was answered based on essay one; possible answers were [Yes, No].

Q2 How prepared and educated do you see yourself in terms of cybersecurity? - This question was answered based on essay three; possible answers were [Extremely, Very, Moderately, Slightly, Not at all].

Q3 Did your view/perception of cybersecurity change over the duration of the

[2] https://niccs.us-cert.gov/about-niccs/glossary

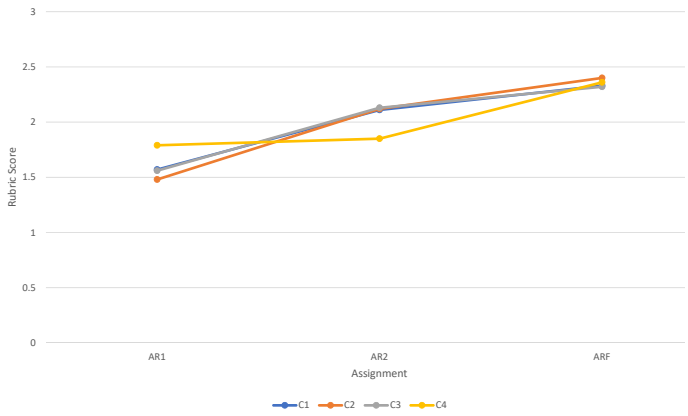


Figure 4. Average cybersecurity knowledge rubric category scores over time.

course? - This question was answered based on essay three; possible answers were [Yes, No].

First, a randomized sample of students was selected for evaluation. A software program was used to return 7-8 students per section; students who missed the first or last essay were replaced. The selected sample was structured to randomize the effect of the section instructors on the outcomes, as the effect of individual instructors is out of the scope of the problem under consideration. Further, one section was graded significantly more leniently than the other seven in the student population by the assigned instructor - this section was considered an outlier and removed prior to analysis. After selection, two individuals were tasked with assessing the data according to the rubric and questions. Several essays were evaluated together to establish a baseline for scoring. Once established, the remaining essays were split between them.

Since the rating of students' work using the rubric was on an ordinal scale, a non-parametric Friedman test was performed on each rubric category, with groups corresponding to academic reflection 1 (AR1), academic reflection 2 (AR2) and the final reflection (ARF). Students with missing scores on a given category were excluded from that analysis. The Friedman test measures whether changes in the scores over time are unlikely to be random. A significant result indicates that a non-random change has occurred in the score being measured across groups. That is, at least some pair of groups has different mean rank.

5.2. Cybersecurity knowledge results

The results of the Friedman tests are summarized below. Fig. 4 gives a visual indication of the estimated means for each rubric category over time. The chart shows across all rubric categories that the average student moved from the area of rubric score 1 (beginning knowledge) to rubric score 2 (developing knowledge). Since the same rubric was used as both an assessment and a teaching tool across a set of three identical assignments, this seems to represents a measurable gain in student ability. We proceed with a statistical analysis that will show numerical evidence for our observations from the chart.

The results show that the differences between the rubric scores over time are significant and unlikely to be random. The statistical summary can be found in Table 4.

As each rubric category shows significant differences over time, we now seek to

Table 4. Friedman test results on significance of rubric category scores over time.

Category	χ^2	p
C1	26.629	.000
C2	40.881	.000
C3	26.567	.000
C4	12.024	.002

Table 5. Differences between mean AR1 and ARF rubric category scores

Category	**AR1**	**ARF**	**Difference**	p
C1	1.57	2.33	0.76	.000
C2	1.48	2.40	0.92	.000
C3	1.56	2.32	0.86	.000
C4	1.79	2.36	0.57	.002

establish that those differences are due specifically to growth in rubric scores. To do so, we proceed with a post hoc Wilcoxon signed-rank test with the Bonferroni correction at the 95% level. Here, we find that for each rubric category, a statistically significant difference exists between the mean scores for AR1 and ARF.

Table 5 indicates that for each rubric category, the average score increased an estimated half a point or more. The confidence intervals give ranges where the expected true increase is likely to fall. The most striking increase is in rubric category C2, where nearly an entire point increase is estimated to have occurred between the first reflection and the final reflection. While these differences might seem marginal, it is important to keep in mind that these are *qualitative* rubrics, and that the largest difference in categories exists between insufficient and emerging. That is, the results indicate a leap of a student showing no evidence of understanding or executing the assignment to a a student that can understand and respond to a college-level prompt. This is particularly striking given that the typical student begins studies at the insufficient level.

We also describe the results of the three questions about the student assignments. Q1 asked if AR1 showed evidence that the student was worried about their online identity. Of all the reflections, 23 indicated *yes*, 21 indicated *no*, and 12 were unable to be scored. Q2 measured the degree to which the final reflection showed how educated students saw themselves in cybersecurity; 0 responses indicated *extremely*, 5 indicated *very*, 12 indicated *moderately*, 18 indicated *slightly*, 0 indicated *none*, and 19 were unable to be scored. Q3 asked if the final reflection indicated that a student's perception of cybersecurity changed over the duration of the course; 40 final reflections indicated a change in awareness around cybersecurity issues, 3 showed no change in awareness, and 8 were unable to be evaluated for various reasons (e.g. wrong content, did not follow directions, etc.). These results are in line with the rubric scores analyzed above, indicating that the majority of students left the class with some improvement, but not high levels of knowledge on average.

6. Limitations

The assessment of the essays was performed manually, which means that human error might have been introduced, e.g., placing an error in an incorrect category or answering a question incorrectly. Furthermore, we encountered a few missing essays where students did not submit the second academic reflection. Several essays did not have sufficient content to answer the questions or to place them in the appropriate category. In particular, for the second academic reflection we found a large number of assignments that did not allow us to categorize them for the portion of the rubric in which we assessed whether students can express personal concerns about technological issues. However, due to the large number of essays that we were able to assess, we believe that our analysis is representative in both breadth and depth.

7. Discussion and Conclusion

We now consider the research questions posed at the top of this manuscript:

[R1] Did adding additional material impact student's performance, i.e., were course outcomes impacted? Interestingly, with regard to question R1, the results in Sec. 4 indicate that the additional material included in the Cyber World classes did *not* hurt student performance - in fact, the opposite appears to be true. Student outcomes were measurably higher in the Cyber sections that in the Non-Cyber sections. Given that student assignment to the Cyber sections was random, and thus no self-selection element should have been present, several explanations seem plausible.

One possibility is that the professors introduced bias into the outcomes - professors with skill and enthusiasm in computer and security issues may have approached their lectures with more energy and enthusiasm than those in the Non-Cyber version of the course. We discussed the possibility that instructors who were unfamiliar with Common Course rubrics and assignments might have graded differently than those who are more well-versed in the course requirements. We did note some differences in grading, but those differences appeared to be confined to specific categories within some of the assignment rubrics. However, half of the instructors teaching in the Cyber sections did not have this specific expertise. Another possibility is that the addition of a thematic through-line in the course provided an organizing principle that the students responded positively to, making the open-ended elements of the course, such as the project proposal and design, easier to envision and grapple with than in the Non-Cyber courses. In any case, it would be interesting to see if other domain-specific content injected into the Common Course leads to similar outcomes.

[R2] Were students able to comprehend the cyber-related material, i.e., did they gain domain knowledge? With regard to question R2, the results in Sec. 5 give strong evidence that students did increase their cybersecurity knowledge. While the rubric scores on average only moved up about one category, for a population starting with almost no knowledge in the area, moving up one category demonstrates a relatively large change over the course of a semester. Note that this increase occurred across a population of students in decidedly non-technical majors (a selection of ten students at random resulted in majors of psychology, criminal justice, forensic science, marketing, and national security). Further, the students' papers as a whole showed strong evidence of a shift in awareness as well as knowledge.

Conclusion & Future work The inclusion of cybersecurity material in the Common Course appears to have been a success, given that both objectives were achieved. Students had higher overall outcomes on Common Course specific objectives and materially increased their cybersecurity knowledge and awareness. The success of this version of the Common Course not only supports the idea that important cybersecurity content can be integrated into the course, but that potentially other versions of the course with important domain knowledge could also be designed.

Acknowledgement(s)

The work reported in this paper was supported by a grant from the Davis Educational Foundation established by Stanton and Elisabeth Davis after Mr. Davis's retirement as chairman of Shaw's Supermarkets, Inc. We acknowledge the following faculty from the University of New Haven who participated in teaching the Cyber World Course: Ibrahim Baggili, Guy-Serge Emmanuel, Michael French, Glenn McGee, and Matthew Schmidt.

Funding

This work was supported by the Davis Educational Foundation. Any opinions, findings, and conclusions or recommendations expressed in this work are those of the authors and do not necessarily reflect the views of the Davis Educational Foundation.

Compliance with Ethical Standards

Ethical Approval. All procedures performed in studies involving human participants were in accordance with the ethical standards of the Human Research Ethics Committee (HREC) and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Informed consent. Informed consent was obtained from all individual participants included in the study.

Conflict of Interest. The authors declare that they have no conflict of interest.

References

Allen, M. (2014). Using rubrics to grade, assess, and improve student learning. *Strengthening Our Roots: Quality, Opportunity & Success Professional Development Day*, 82.

Breitinger, F., & Nickel, C. (2010). User survey on phone security and usage. In *Biosig* (pp. 139–144).

Brookhart, S. M., & Chen, F. (2015). The quality and effectiveness of descriptive rubrics. *Educational Review*, *67*(3), 343-368.

Das, A., Voorhees, D., Choi, C., & Landwehr, C. E. (2017). Cybersecurity for future presidents: An interdisciplinary non-majors course. In *Proceedings of the 2017 acm sigcse technical symposium on computer science education* (pp. 141–146).

Dawson, P. (2017). Assessment rubrics: towards clearer and more replicable design, research and practice. *Assessment & Evaluation in Higher Education*, *42*(3), 347-360.

Dupuis, M. J. (2017). Cyber Security for Everyone: An Introductory Course for Non-Technical Majors. *Journal of Cybersecurity Education, Research and Practice*, *2017*(1), 3.

Educause. (2018, December). *Top 10 IT Issues, Technologies, and Trends.* (https://www.educause.edu/research-and-publications/research/top-10-it-issues-technologies-and-trends)

Edwards, J. B. (2018). Added value or essential instruction?: Librarians in the twenty-first-century classroom. *Reference & User Services Quarterly*, *57*(4), 285–293.

Gibson, C., & Jacobson, T. E. (2018). Habits of Mind in an Uncertain Information World. *Reference & User Services Quarterly*, *57*(3), 183–192.

Haigh, R. W. (1985). Planning for computer literacy. *The Journal of Higher Education*, *56*(2), 161–171.

Heinricher, A. (2019). Introduction: A Little Bit of History. In K. Wobbe & E. A. Stoddard (Eds.), *Project-Based Learning in the First-Year: Beyond All Expectations* (pp. 13–18). Stylus Publishing.

Hendler, J., Shadbolt, N., Hall, W., Berners-Lee, T., & Weitzner, D. (2008). Web science: an interdisciplinary approach to understanding the web. *Communications of the ACM*, *51*(7), 60–69.

Johnston, B., & Webber, S. (2003). Information Literacy in Higher Education: a review and case study. *Studies in Higher Education*, *28*(3), 335-350.

Karkehabadi, S. (2013). *Using rubrics to measure and enhance student performance.* Retrieved last accessed 2019-09-07, from https://www.nvcc.edu/assessment/_docs/FTW5.usingrubricsmeasurestuperf-spr13.pdf

Korovessis, P., Furnell, S., Papadaki, M., & Haskell-Dowland, P. (2017). A toolkit approach to information security awareness and education. *Journal of Cybersecurity Education, Research and Practice*, *2017*(2), 5.

Nager, A., & Atkinson, R. (2016, May). The case for improving US computer science education. *Information Technology & Innovation Foundation*. (http://www2.itif.org/2016-computer-science-education.pdf)

National Resource Center. (2019). *About Us: Mission Statement.* https://sc.edu/about/offices_and_divisions/national_resource_center/about/index.php. University of South Carolina.

Office of Insttitutional Research and Assessment at the University of North Carolina. (2017, July). *Using rubrics to assess student learning outcomes at the program level.* Retrieved last accessed 2019-09-07, from https://oira.unc.edu/files/2017/07/Developing-and-Using-Rubrics.pdf

Ponemon Institute. (2018, Oct). *2018 cost of Data Breach Study: Impact of Business Continuity Management* (Tech. Rep.). Ponemon Institute. Retrieved from https://www.ibm.com/downloads/cas/AEJYBPWA

Przyborski, K., Breitinger, F., Beck, L., & Harichandran, R. (2019). "cyberworld" as a theme for a university-wide first-year common course. *ASEE Annual Conference & Exposition*.

Ragupathi, K., & Lee, A. (2020). Beyond fairness and consistency in grading: The role of rubrics in higher education. In C. S. Sanger & N. W. Gleason (Eds.), *Diversity and inclusion in global higher education: Lessons from across asia* (pp. 73–95). Singapore: Springer Singapore. Retrieved from https://doi.org/10.1007/978-981-15-1628-3_3

Reddy, Y. M., & Andrade, H. (2010). A review of rubric use in higher education. *Assessment & Higher Education*, *35*(4), 435 – 448.

Ricci, J., Breitinger, F., & Baggili, I. (2018, 7). Survey results on adults and cybersecurity education. *Education and Information Technologies*, 1–19. Retrieved from https://doi.org/10.1007/s10639-018-9765-8

Smith, B. F., & Brackin, R. (1993). Components of a comprehensive orientation program. *Designing successful transitions: A guide for orienting students to college*, 35–48.

Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015). Cyber education: a multi-level, multi-discipline approach. In *Proceedings of the 16th annual conference on information technology education* (pp. 43–47).

Stiller, E., & LeBlanc, C. (2006). From computer literacy to cyber-literacy. *Journal of Computing Sciences in Colleges*, *21*(6), 4–13.

Tavani, H. T. (2002, Fall). Applying an interdisciplinary approach to teaching computer ethics. *IEEE Technology and Society Magazine*, *21*(3), 32-38.

Upcraft, M. L. (1993). Orienting today's students. *NOTE 213p. AVAILABLE FROM University of South Carolina, The Freshman Year Experience, 1728 College Street, Columbia, SC 29208*, 1–8.

Werner, L. (2005). Redefining computer literacy in the age of ubiquitous computing. In *Proceedings of the 6th conference on information technology education* (pp. 95–99).

Appendix A. Rubric

Table A1. Rubric used to evaluate project proposal.

Criteria	**Levels of Achievement**			
	Insufficient	Emerging	Proficient	Exemplary
Description (20%)	Description of experiences, summary of text, or explanation of concepts is not clear, sufficient, and factually correct.	Description of experiences, summary of text, or explanation of concepts is lacks clarity, sufficiency, and accuracy.	Description of experiences, summary of text, or explanation of concepts is mostly clear, sufficient, and factually correct.	Description of experiences, summary of text, or explanation of concepts is clear, sufficient, and factually correct.
Analysis (30%)	Connections are not made between course concepts and/or experiences. Very little to no evidence is used or analyzed. Only addresses one point of view.	Connections are suggested between course concepts and/or experiences. Some ideas are supported with reliable evidence. Does not specifically address more than one point of view.	Connections are made between concepts and/or experiences but may lack detail. · Most ideas are supported with attributed, reliable evidence. More than one point of view is considered, acknowledging the complexity of the issue.	Specific connections are made between concepts and/or experiences.· Ideas are supported with clearly attributed evidence that is demonstrated to be reliable. The complexity of the issue is acknowledged as multiple perspectives are analyzed.
Conclusions (30%)	The paper does not clearly draw conclusions or discuss what has been learned from the experience.	The paper draws conclusions that are not based on the evidence provided. It is not clear how the student has learned from the experience.	The paper draws relevant conclusions that are linked to the evidence. The paper also discusses what the student has learned from the experience.	The paper draws specific, relevant, and logical conclusions that follow from the analysis of the evidence. It is clear how the student has learned from the experience.
Style (10%)	The paper does not express a clear core idea. Ideas are not organized logically. Little to none of the paper is written in an academic tone. Little to none of the aspects of the assignment are followed.	The paper expresses a core idea at the beginning, but the idea does not follow through. Ideas are organized somewhat logically. Some of the paper is written with an academic tone. Some aspects of the assignment are followed.	The paper is focused on a core idea that appears through the paper. Ideas are organized logically and, for the most part, transition smoothly between sentences and paragraphs. The paper maintains an academic tone through most of the paper. Most aspects of the assignment are followed.	The paper is focused on a core idea that effectively follows through the paper. Ideas are organized logically and transition smoothly between sentences and paragraphs. The paper maintains an academic tone. All aspects of the assignment are followed.
Professionalism (10%)	The spelling, punctuation, and grammatical errors make the paper very difficult to read. The paper is not formatted in MLA 8 and/or the Works Cited page and in-text citations (if applicable) are missing.	The paper has significant spelling, punctuation, and grammatical errors. The paper has many errors in MLA 8 formatting (including Works Cited and in-text citations if applicable).	The paper has few spelling, punctuation, and grammatical errors. MLA 8 formatting is adhered to, though with a few errors (including Works Cited and in-text citations if applicable).	The paper is free from spelling, punctuation, and grammatical errors. MLA 8 formatting is adhered to (including Works Cited and in-text citations if applicable).