”Cyber World” as a Theme for a University-wide First-year Common Course

Dr. Kristen Przyborski, University of New Haven

Kristen Przyborski is the Common Course Director and a Lecturer in the Department of Biology and Environmental Science at the University of New Haven. Her PhD is in Biological Oceanography from the University of South Florida. The focus of her doctoral studies was the ecology of natural toxins. The pedagogy of science, critical thinking, and scientific literacy are her primary research interests today.

Dr. Frank Breitinger, University of New Haven

Dr. Frank Breitinger received the B.S. degree in computer science from the University of Applied Sciences in Mannheim (2009, Germany), his M.S. degree in computer science from the University of Applied Sciences Darmstadt (2011, Germany) and his Ph.D. degree in computer science from the Technical University Darmstadt (2014). He was self-employed for 5 years, a visiting researcher at the National Institute of Standards and Technology to lead NIST SP 800-168 on Approximate Matching, and interned as a software developer for the University of Maryland and the sobedi GmbH (Mannheim, Germany). Since 2014 he is an Assistant Professor of computer science at the Tagliatela College of Engineering at the University of New Haven, CT (ECECS department) with a research focus on cybersecurity and digital forensics. He has published numerous peer-reviewed articles, chaired an international conference in cybersecurity in Manhattan and serves as a reviewer on several program committees. Additional information about him and his work is on his website: https://www.FBreitinger.de.

Dr. Lauren Beck, University of New Haven

Lauren Beck 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.

Dr. Ronald S. Harichandran, University of New Haven

Ron Harichandran is Dean of the Tagliatela College of Engineering and is co-PI of the grant entitled Development of the ’CyberWorld’ Common Course at the University of New Haven that facilitated the work reported in this paper.

‘Cyber World’ – A Cybersecurity Theme for a University-Wide First-Year Common Course

Abstract

While living in a cyber-connected society provides students with unprecedented connectivity and convenience, it also has the potential to expose them to a variety of threats and manipulations. Internet security on college campuses has become a primary concern of those tasked with protecting campus networks. We developed a “Cyber World” version of our team-taught first-year experience course at the University of New Haven with the intent of introducing students to important cybersecurity concepts. In comparison with other topics taught during the same semester, students reported a greater level of knowledge in topics of identity theft, safe practices for online transactions, fake news, and information oversharing. A pilot online module related to lectures and class activities was well received and supports the increased use of online modules in future semesters. Students’ self-selected project topics indicate that in future semesters the topics explored in lecture should be expanded beyond cybersecurity issues to include social media topics, particularly cyberbullying body image issues.

Introduction

Cybersecurity is a growing concern for both the private sector and governments. It has enormous implications for government security, economic prosperity and public safety. The number of data breaches in the education sector doubled during 2017, with only the financial and healthcare sectors having more breaches [3]. The cost of a data breach in U.S. education is higher than the cost in other sectors and countries [18]. Domains with “.edu” addresses are a high risk for data breaches due to their value on the Dark Web [5]. It is not surprising then that IT professionals rated information security as the top concern for three years in a row [7]. Additionally, it is also a concern for parents who are worried about their children losing their identity [19].

On the other hand, students spend a lot of time online; 95% of teens aged 13-17 have smartphones, and 45% of teens report being online almost constantly [1]. The vast majority of Americans in the 18-24 year age range report using social media, particularly Youtube (91%), Facebook (80%), Instagram (71%), and Snapchat (78%) [1]. However, according to an online poll conducted by the Pew Research Center [17], people 18-29 years old on average only answered 6 out of 10 cybersecurity relates questions correctly. This age group has performed particularly poorly on subjects related to encryption, such as whether Wi-Fi traffic is encrypted by default.

Despite the amount of time spent online by this demographic and the potential impact of data

breaches in higher education, the efforts of information technology staff on college campuses to alert students of data breaches is largely unsuccessful. Few students are aware of communications involving these efforts. Furthermore, there is an apparent disconnect between the amount of training that students state they receive on cybersecurity issues versus the amount of training IT staff believe the students are receiving [14].

As a consequence, we decided to 'create'[1] a course named *Cyber World* at the University of New Haven. The course focused on different aspects of cyber-related issues such as protecting against identity theft, safe practices for online transactions, fake news, and information oversharing. The course was taught to about 160 first-year undergraduates and allowed interdisciplinary collaboration between faculty.

Our paper has three significant contributions: (1) We present the eight topics related to living in a Cyber World that we chose for this course, including our rationale for why they are appropriate and relevant (see section Lecture Overview); (2) We summarize how we integrated the Cyber World topics into the structure of the Common Course; and (3) We summarize some initial results on how students as well as faculty perceived their experience, and how they performed compared to other common course sections/topics. The last two sections include discussions of the challenges we faced as well as the conclusion and future directions.

Literature Review

While highly technical courses in cybersecurity are essential for students training for a career in the field, there exists a broader need for non-majors to understand the basics of cyber dangers and protections from them. Although all of our students regularly use the internet and may be somewhat aware of dangers and security risks, most do not know how to protect themselves and act responsibly in many online situations [13].

There are arguments that courses in computer science should be considered a core science course taught as a general education requirement and required for all students [16]. In the article, 'Planning for Computer Literacy', Roger W. Haigh [10] discusses how colleges and universities would need to decide what computer literacy skills students would need for their careers and personal lives. Since then, universities have offered a variety of general education courses in computer literacy and programming. Some existing courses that are part of the core focus on highly technical skills, while others are aimed at educating students more generally. Recently, there has been a call for an expansion of computer literacy to include cyber literacy, safety, and security [21, 22, 24]. Universities have begun to offer courses in cybersecurity specifically designed for non-majors because of the way that cybersecurity issues impact the everyday individual as well as people in all areas of employment (finance, corporate, government, military, healthcare, etc.). Loyola University in Maryland[2] offers a 'Cyber Security and Digital Forensics' course that focuses on the basics of cybersecurity measures. University of Washington, Bothell offered a cybersecurity course for non-majors that included a lab section, teaching students

[1] Specifically, we developed the course materials and modified our common course as outlined in Overview of the Common Course.

[2] https://www.loyola.edu/academics/computer-science/degrees/non-majors (last accessed 2019-01-27).

technical skills, such as installing protective software, and teaching students how to regularly backup information to the cloud [6]. At Le Moyne College, an interdisciplinary non-majors course was offered titled 'Cybersecurity for Future Presidents.' This course, like the one at Loyola, taught students technical skills like encryption, decryption, and packet switching [4].

The non-majors courses in cybersecurity that have been designed vary greatly in the style and content [6]. Some of the topics covered in these courses are similar to ours: computer networks, cryptography, access controls, threats and human factors, forensics, privacy, ethics, and free speech, and other computer science fundamentals like, digital representation of information, data encryption, time complexity, packet switching networks, distributed computing and big data sets [4].

An important aspect of cybersecurity for the everyday person is a strong set of information literacy skills. Librarians and other information specialists have indicated a pressing need for courses that promote understanding of the reliability of information, especially on the web where expertise is often difficult to determine [8, 9]. First-year seminars as well as critical thinking and project-based courses are places where this type of learning objective is addressed because of a general agreement that students need information literacy skills to be successful throughout college. Collaborations between librarians and instructors have been documented as being essential to the success of students navigating complex information resources [2, 12, 15]. In our course, a librarian was brought in as a ninth specialist in information literacy in addition to the presentations given by the eight instructors in our course. This type of literacy was explicitly linked to cyber literacy as we highlighted the ways that skills in detecting authority and bias were essential to behaving safely in an online environment.

While some of the courses discussed above indicated that they were interdisciplinary, there is no evidence of courses that include instructors from outside of the computer science discipline. The literature suggests a desire for more interdisciplinary collaboration, since the Cyber World is one that continually evolves through human behavior. Thus, theories and lessons from various disciplines may be useful in understanding cybersecurity [11]. Additionally, in teaching students to navigating ethical concerns and human deception, both technical and humanistic expertise may be required of instructors [23]. The Common Course at our university is designed as an interdisciplinary course that teaches skills—critical thinking, problem solving, team work, and effective communication—applicable to all fields. This style is what Rives-East and Lima [20] call 'transdisciplinary', meaning that the course transcends any specific discipline. Cyber World, however, with its foundation in the sciences, used a model closer to Rives-East and Lima's 'jigsaw' in which faculty from various disciplines establish their own specialty on the topic relating to their subject expertise.

Overview of the Common Course

In Fall 2018, we initiated a pilot course that would bring a discussion of cyber-related topics into our first year critical thinking course, which we refer to as the Common Course. This serves as the only core critical thinking course that all students at the university are required to take in their first year. The primary purpose of the course is to ensure students have the information literacy

and academic research skills to succeed in college. The course employs a model that uses 8 instructors from across the university to teach an interdisciplinary course around a common theme to approximately 160 students. Previous themes have included Happiness, Identity, Justice, and Politics.

The emphasis of the course on information literacy and the connection between digital literacy and information literacy provides an opportunity to explore topics of a more technical nature that are relevant to students' ability to make connections between their actions online and the impact on their own lives. In addition to skills related to research and information literacy, we decided to introduce a new theme named *Cyber World* with the expectation that students would come away from the class with specific cyber-related knowledge. A special challenge in regards to a STEM oriented topic such as this is that students who take the course are by design from all majors represented on campus. Specifically, 808 students from 48 majors enrolled in the course in Fall 2018 (see Table 1 for breakdown by majors). Of these students, most were from Forensic Science, Criminal Justice, and Psychology. Concurrently offered Happiness and Identity topics provided a means of comparing students experience in the course as well as their ability to evaluate credible sources and perform academic research.

Table 1: Student demographics.

Program	**Student #**	**Program**	**Student #**
Forensic Science	217	Graphic Design	13
Psychology	88	Interior Design	12
Criminal Justice	81	Paramedicine	11
Biology	62	Health Sciences	10
Music & Sound Recording	37	Nutrition and Dietetics	10
Dental Hygiene	32	Sport Management	10
National Security	26	Marketing	8
Business Management	24	Cybersecurity	7
Music Industry	23	Communication	6
Engineering	22	Computer Science	6
Fire Science	15	Undeclared	32
Marine Biology	15	Other	41

The structure of the course is based on two contact sessions per week as well as a group project. The "Whole Group Session" consists of 4 sections meeting together in a large lecture hall for one class period a week. On the second class day of the week, students meet in breakout sessions with their individual instructors to discuss whole group topics and work on skills related to course outcomes. The course is taught in clusters of 8 sections, taught by eight faculty members from different colleges having expertise in a variety of disciplines. An important side effect of this faculty diversity is that interdisciplinary collaborations among faculty are promoted.

Lecture, active discussion, and group problem solving activities are used extensively, with a strong emphasis on active student learning. The emphasis of assignments are to provide students opportunities to develop an understanding and apply newly learned theory, principles, and practices using written and verbal forms of communication. A major part of the course is a group project presented to the campus community in the final week of classes. Faculty from all colleges

on campus evaluate students' ability to develop a polished pitch and summarize their project succinctly with an academic poster.

Lecture Overview

Before working on the outline of the course, we asked ourselves if we should identify topics first and then contact appropriate/interested faculty or vice versa. We decided that it was most important to have motivated and engaging faculty members for the course; on the other hand, we believed that every faculty member can relate their area of expertise to the Cyber World. Hence, after forming our instructor-team, we sat down to find overlaps between their areas of expertise and cyber issues. This resulted in a lecture series of 8 topics developed and delivered by faculty from four colleges: the College of Arts and Sciences, the College of Business, the Tagliatela College of Engineering, and the Henry C. Lee College of Criminal Justice and Forensic Science.

Each of the topics is summarized below and reflects the instructor's expertise under the umbrella of Cyber World (topics are in order):

1. *Digitization, Artificial Intelligence & Command Control* – Focused on binary, electromagnetic modulation for binary data transmission and systems control, and implications of these capacities in the context of modern computing, the internet and robotics (e.g., impact of drones during warfare). Also, methods of analog information manipulation in the Soviet system were discussed and as amplified by the modern tools discussed above.

2. *The Performance of Truth* – Discussed the credibility of Internet sources. Students were asked to examine the credentials, motivation, and sponsorship of bloggers to determine reliability. In analyzing the ways that some blogs manipulate readers' emotions, hide corporate sponsors, and cite unreliable sources, students were able to learn skills that could be applied to other online sources.

3. *Cyber Forensic Science: Should there be a backdoor to encryption?* – Discussed what cyber forensic science is, how data may be recovered from digital devices, and the privacy implications when data is not fully deleted from devices and the network on which they reside. Students also debated the ethical implications of building a backdoor into personal devices for use by law enforcement agencies.

4. *Noone Knows Who You Are in the Cyber World, Not Even You: How the Internet changes your identity* – Discussed ethical, legal and business implications of personal digital identity for individuals and society at large. Students examined the degree to which their online identity reflects who they think they are, and examined the different versions of themselves present in different forms of Internet activity, e.g., LinkedIn, Facebook, Snapchat, dating apps, etc.

5. *Ethics and Artificial Intelligence* – Discusses artificial intelligence and ethical issues surrounding its use. A key in-class exercise was the comparison between artificial intelligence and human intelligence through a Turing test (i.e., AI chatbots versus three instructors) followed by a discussion on what artificial intelligence is. This led to questions such as what does it mean to be intelligent, is artificial intelligence a threat, and how should we treat/engage with artificial intelligence.

6. *Who Owns the Digital You?* – Discussed the problems and impacts of digitization of genetic information (e.g., 23andMe.com), and the ease with which genetic information can be sequenced and how this information can be analyzed and stored digitally. Several well-known case studies in which individuals had their genetic data compromised were compared with situations in which the use of genetic data resulted in a greater public good.
7. *Social Engineering and the Power of Graphic Design in an Online Environment* – Explored social engineering and graphic design in relation to an online environment. Social engineering, in the context of information security, refers to psychological manipulation of people so that they perform specific actions or divulge confidential information. Students were introduced to how graphic design can influence the reader and viewer into making a decision.
8. *Cybersecurity Principles: How can I protect myself against attacks?* – Discussed how students can protect their personal digital devices and recommend methods by which they can protect themselves online. Additionally, students learned about personally identifiable information (PII), and why it is important to protect it (identity theft). Finally, students participated in exercises on the importance of choosing strong passwords, avoiding phishing websites, and recognizing disguised spam emails.

Besides two of the instructors, none of the faculty was particular familiar with cybersecurity. Thus, faculty learned with the students, which ensured that lectures were not too technical and were easy to understand for first-year students.

Integrating Cyber World into the Common Course

The Common Course in its current form started in Fall 2015 and was in its 6^{th} iteration. Thus, the course structure was well defined and administrators had achieved a balance between instructor autonomy and a more structured approach that ensured instructor confidence in course delivery. Regardless of the theme, sections used identical rubrics, similar assignments and basic course materials. In the case of Cyber World, materials were modified to include pre and post quizzes to ensure student engagement with the material. Having a clear structure, we aligned the topics based on the corresponding assignments. For example, the topic "Cyber Forensic Science: Should there be a backdoor to encryption?" was offered during the 7^{th} week of the semester so as to align with a mid-semester academic reflection. The integration of the 8 faculty topics into the existing common course structure was no more difficult than it was for non-STEM topics.

Evaluation Results

Much of the data collected in this initial semester were qualitative in nature. We attempted to answer the following questions through the use of surveys:

1. How did students and faculty rate the quality of the educational experience?
2. What were the perceived successes?
3. What needs to be improved, why, and how?

Student thoughts about the quality of the course: We examined the course evaluations of students in the Cyber World sections with those in the two other topics offered during the same semester. One common set of questions was used for all courses, and the survey was administered electronically. The results are summarized in Table 2. Overall course evaluation completion rate for students taking the Common Course in Fall 2018 (n = 808) was 83%. Cyber World sections received higher evaluations for the majority of the questions on the course evaluations. Results of the t-test show a statistically significant mean difference between Cyber World sections and other sections in questions relating to instructor quality as well as course specific questions. In all, 10 out of the 14 course evaluation questions were rated higher by students in Cyber World than in Happiness or Identity.

Table 2: Course Evaluation results from our end of the semester survey.

		Other sec. n = 537		Cyber sec. n = 117					
	Course evaluation questions	**M**	**SD**	**M**	**SD**	**df**	***t*-stat**	***p*-value**	
1	The objectives of the course were clear.	2.46	1.24	2.72	1.23	171	2.02	0.04	*
2	The course materials (as listed on the syllabus) contributed to my learning.	2.53	1.19	2.69	1.23	167	1.32	0.19	
3	Assignments and other graded activities gave me an opportunity to demonstrate what I learned.	2.69	1.25	2.95	1.30	166	2.00	0.05	
4	The grading system for the course was clear.	2.97	1.30	2.51	1.44	160	3.16	0.00	*
5	The instructor was prepared for each class.	3.71	1.12	3.91	1.11	171	1.68	0.09	
6	The instructor's presentations were understandable.	3.54	1.20	3.95	0.99	197	3.87	0.00	*
7	The instructor provided helpful feedback.	3.60	1.25	3.86	1.07	188	2.34	0.02	*
8	The instructor used class time effectively.	3.51	1.25	3.92	1.02	200	3.81	0.00	*
9	My interest in the subject matter was enhanced by the instructor's enthusiasm.	2.87	1.34	3.36	1.30	174	3.71	0.00	*
10	The instructor raised questions or problems that encouraged me to think critically.	3.25	1.27	3.62	1.18	179	3.06	0.00	*
11	The instructor explained the relevance of the subject matter.	3.11	1.28	3.68	1.11	189	4.91	0.00	*
12	The instructor established a positive learning environment.	3.71	1.18	4.06	0.88	218	3.64	0.00	*
13	The instructor was accessible outside of class (for example: held office hours, communicated via email, or offered to meet via video conferencing).	3.75	1.12	3.91	1.00	186	1.57	0.12	
14	Overall, I was satisfied with the educational experience provided by the instructor.	3.27	1.30	3.61	1.21	180	2.66	0.01	*

M=mean; SD=standard deviation and * indicates statistically significant at the 95% confidence level.

Faculty thoughts about the quality of the course: In addition to students' input, we also asked instructors for their feedback. Most instructors agreed that teaching the Cyber World course to freshmen was relevant and enjoyed it. Furthermore, the group enjoyed the team teaching aspect and teaching outside of their domain. Even instructors who had taught the Common Course before found this to be one of the most engaging and successful themes, largely due to its pragmatic application for the students (this is reinforced by the evaluations for different sections of the Common Course). On the flip side, some faculty felt that the team needed to be more

cohesive, while others felt that some members of the team did not allocate sufficient priority to the Cyber World course. Some faculty also underestimated the amount of grading that comes with the course (there are many homework assignments, exercises and presentations). Lastly, some faculty felt that students came in with a bias toward the course which made teaching the class challenging.

Representative responses:

"After teaching in the Cyber World section I'm absolutely convinced this is a critical need for contemporary students. I was shocked at how little understanding students who were otherwise grafted to electronics understood about the technology itself and, more importantly, the social and political implications of that technology."

"I found the Cyberworld project to be a fascinating one. I'd like to begin by saying that it was an incredible experience for myself regarding pedagogy. I learned a lot about teaching from sharing the classroom with an array of high-level instructors. The team-teaching model worked well for me."

"I thoroughly enjoyed teaching the Cyber World class. As a cybersecurity professor, I truly enjoyed passing on the knowledge to non-cyber majors, especially given that my field has a huge workforce shortage. Many of the students were so intrigued by our small group discussions, and some thought they may want to switch majors to cybersecurity and computer science."

"I established stronger relationships with faculty from other disciplines, and I felt that all of the instructors for the course benefited from learning more about the purpose of the common course as well as student experience in the course."

"I would have liked more collaboration among the instructors. [...] I think we could have been more innovative, interdisciplinary, and effective at getting students enthusiastic. ‘’

"My biggest critique was that the topics of the larger group lectures were hard to bring up for any serious discussion in the small groups because of the focus on completing the group project. This left a sense that the large group lectures were separate from the small groups.‘’

Online module reflection questions: The effectiveness of the pilot online module was assessed via a question in the final reflection. Students were asked to reflect upon the effectiveness of the module in understanding the topic better, the duration, length and materials included in the module, and whether the inclusion of additional modules would enhance the course. 88 students opted to complete the question on the final exam. Of those 88 students, 73% indicated that they thought the module was useful in helping them to understand basic cybersecurity concepts and that online modules should be used more throughout the course.

Representative responses:

"I feel like I learned the most practical information about cybersecurity within the module. I would have liked to learn more information like this in the rest of the course."

"If we did more of these modules to cover the content in the class, I think that it would help with understanding the content and overall help with the understanding of the importance of this course."

"The online module on cybersecurity was very interesting and held my attention. It did help increase my knowledge on the topic, and it was very helpful to have an additional online component to the course as well as in person."

"I believe that the online module was exceptionally powerful and engaging in terms of getting the basics of cybersecurity across to a complete novice."

Those students who did not find the modules helpful consistently stated that they were not comfortable with online learning in general.

"I don't think modules are ever an efficient way to teach students pertinent information."

"It's sometimes hard to understand these social topics through the internet and reading materials because it's not mostly a visual learning experience instead of an approach that caters to multiple learning styles."

"I would rather hear true stories from professors in class than watch videos and do modules outside of class. I pay more attention when in class and discussions with others in class made the lessons easier to understand."

Focus groups: End of semester focus groups were conducted with students to assess their perceptions of the academic experience. The following common themes from the groups emerged:

- Students would have preferred to see greater depth with individual topics, even if it meant reducing the number of topics discussed.
- Students reported having much more knowledge of password security and an enhanced ability to spot fake websites.
- Students reported a dearth of scholarly resources in cybersecurity issues when researching their group projects.
- The diversity of faculty backgrounds and diversity in faculty topics resulted in a better understanding of how cybersecurity could relate to other fields.
- Students enjoyed the faculty presentations and indicated that they would like to see more of this in future courses.

Discussion and Road Blocks

Overall, our qualitative assessments revealed that although there were many aspects of the course that could be deemed a success, there were also other components of the course that should be improved. In the following we discuss some of the challenges we encountered as well as some of the changes we will make in the future.

Variety in Cyber background. Instructors and students came from different backgrounds (knowledge about Cyber topics varied) which made it challenging to create lectures, but also interesting. First, some of the instructors had difficulties relating their expertise with Cyber World and required discussions with cyber experts. For instance, it was challenging to find a topic for

our arts and science faculty (with a background in communications). After several meetings, appropriate topics were identified and educators were able to create their own materials without any additional help. In the aforementioned case we ended up with "Social Engineering and the Power of Graphic Design in an Online Environment" (see section Lecture Overview). On the other hand, the students' knowledge/background were varied as well, e.g., some had already a sophisticated knowledge about cybersecurity and a good vocabulary, while others were starting from the beginning. Thus, it was difficult to find an appropriate starting point for the lectures. To counteract, we decided we would not only have online modules to inform faculty, but would also require students to complete the appropriate module before each lecture to bring them all to the same knowledge base so that lectures could be more advanced. As briefly discussed in the results section, students enjoyed the pilot online learning module. Moreover, from an instructor's perspective, the modules would allow them to better plan a lecture since they could assume that all students would have the same prerequisite knowledge.

Unfamiliarity with course structure. The majority of the instructors had not taught the course before and therefore it was challenging and time consuming to meet weekly and discuss next steps. Surprisingly, these meetings were not about the cyber topics, but covered more general issues such as how the course was structured and what activities were to come next. We believe that this is a result of co-teaching as well as unfamiliarity with the course and not a result of the theme. Ensuring that each team of four faculty members included a team leader who had taught the course before ameliorated the anxiety of new faculty to some extent, but there was often a disconnect between the purpose of the course as the team leaders saw it and the purpose of the course as the other Cyber World instructors saw it.

Online module. A challenge with the Common Course is the fluctuation of faculty from semester to semester. The expertise of individuals is always changing. In order to sustain the Cyber World theme as instructors change in the future, most of the content related to the expertise of the initial developers/instructors will be packaged into e-learning modules that will support the lectures. Originally we were unsure about the online modules and how students would like them as they would require students to do additional work. However, the pilot online module created for the last lecture (Cyber Security Principles: How can I protect myself against attacks?), which can be completed within 45-60 minutes, was well-received by students. The module was developed after the instructor completed a 1-week online training course developed by the Office of E-Learning at the University. It is clear from student responses to the online module that we should include more modules when the course is offered again in the coming year. We anticipate having an online module to accompany each Cyber World topic that is presented.

Conclusion and Future Direction

Although the importance of cybersecurity training for students on college campuses is clear, there is a significant challenge in finding a way to reach students early in their college careers. Offering a cybersecurity related course with academic credit that will be delivered to non-majors is a novel concept for enhancing students' cyber awareness. While the course we developed shows promise, there is still much to be accomplished in terms of merging a critical thinking skills based course

with a content heavy topic such as cybersecurity. However, the effect that this course had on students suggests that the merging of these two concepts holds promise.

Including faculty from multiple academic disciplines can result in students having a better understanding of how cybersecurity intersects with multiple disciplines. For example, students majoring in Genetics and Biotechnology were intrigued by the discussion of genetic information and privacy. Successes such as this indicate that incorporation of cyber-related topics into introductory major specific courses could also be promising.

The development of online modules by individual faculty teaching the course also seems a promising way to deliver cyber-related information to undergraduate students. Each of these self contained modules can be made available to instructors within a field of expertise to adapt for their own classes.

In future semesters we intend to supplement our faculty presence with guest speakers from other areas of campus or from the broader community. By broadening our interactions with the entire campus we will expand our course content to include connections between cyber and other disciplines, thereby enriching and diversifying our students' experiences. From an instructor's point of view, we will encourage faculty to focus even more on their discipline and how it can be used as a weapon or be exploited. So the art teacher could talk about steganography (used as a weapon) and maybe social engineering using differences in culture (weakness in discipline based on a poor understanding of art)[3].

Acknowledgments

This research was funded by the Davis Educational Foundation (DEF). Their support is gratefully acknowledged. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the DEF. Additionally, we would like to thank faculty members Ibrahim (Abe) Baggili, Glenn McGee, Guy-Serge Emmanuel, Matthew Schmidt, Michael French, and John Christie for their support in developing and teaching the first offering of Cyber World.

References

[1] M. Anderson and J. Jian. Teens' social media habits and experiences. http://www.pewinternet.org/2018/11/28/teens-social-media-habits-and-experiences/, November 2018.

[2] C. Boff and K. Johnson. The library and first-year experience courses: A nationwide study. *Reference Services Review*, 30(4):277–287, 2002.

[3] J. Bolkan. Education Data Breaches Double in First Half of 2017. https://thejournal.com/articles/2017/09/20/education-data-breaches-double-in-first-half-of-2017.aspx, September 2017.

[3] This example was provided by a reviewer.

[4] A. Das, D. Voorhees, C. Choi, and C. E. Landwehr. Cybersecurity for future presidents: An interdisciplinary non-majors course. In *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education*, pages 141–146. ACM, 2017.

[5] Digital Citizens Alliance. Cyber criminals, college credentials, and the dark web: A security challenge facing US university communities. https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DigitalCitizens_CollegeInfoTheft.pdf, March 2017.

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

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

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

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

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

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

[12] T. E. Jacobson and B. L. Mark. Separating wheat from chaff: Helping first-year students become information savvy. *The Journal of General Education*, 49(4):256–278, 2000.

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

[14] C. Lestch. College IT experts and students have opposing views on cybersecurity. https://edscoop.com/college-it-experts-and-students-have-opposing-views-on-cybersecurity/, November 2017.

[15] J. Lindstrom and D. D. Shonrock. Faculty-librarian collaboration to achieve integration of information literacy. *Reference & User Services Quarterly*, 46(1):18–23, 2006.

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

[17] K. Olmstead and A. Smith. What the Public Knows About Cybersecurity. http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/, March 2017.

[18] Ponemon Institute. Cost of a Data Breach Study 2018. *Security Intelligence*, 2018.

[19] J. Ricci, F. Breitinger, and I. Baggili. Survey results on adults and cybersecurity education. *Education and Information Technologies*, pages 1–19, 7 2018.

[20] D. Rives-East and O. K. Lima. Designing interdisciplinary science/humanities courses: challenges and solutions. *College Teaching*, 61(3):100–106, 2013.

[21] E. Sobiesk, J. Blair, G. Conti, M. Lanham, and H. Taylor. Cyber education: a multi-level, multi-discipline approach. In *Proceedings of the 16th Annual Conference on Information Technology Education*, pages 43–47. ACM, 2015.

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

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

[24] L. Werner. Redefining computer literacy in the age of ubiquitous computing. In *Proceedings of the 6th conference on Information technology education*, pages 95–99. ACM, 2005.