2021 ASEE ANNUAL CONFERENCE
Virtual Meeting | July 26–29, 2021 | Pacific Daylight Time
Paper ID #32508

Development of a HyFlex Defensive Security Course

Dr. Jeremy Straub, North Dakota State University

Jeremy Straub is the Director of the NDSU Institute for Cyber Security Education and Research and an Assistant Professor in the Department of Computer Science at the North Dakota State University. He holds a Ph.D. in Scientific Computing, an M.S. and an M.B.A. and has published over 40 journal articles and over 120 full conference papers, in addition to making numerous other conference presentations. Straub's research spans the gauntlet between technology, commercialization and technology policy. In particular, his research has recently focused on cybersecurity topics including intrusion detection and forensics, robotic command and control, aerospace command and 3D printing quality assurance. Straub is a member of Sigma Xi, the AAAS, the AIAA and several other technical societies, he has also served as a track or session chair for numerous conferences.

Development of a HyFlex Defensive Security Course

Abstract

A flexible learning defensive security course was developed using the HyFlex delivery model which was initially developed at San Francisco State University. This paper discusses how a limited-flexibility model was transformed due to the COVID-19 pandemic and how the course was changed from having a single path to offering a HyFlex Options Menu where students select between several options for each area of the class. The overall outline and instructional design of the course are presented. The implementation of each of the HyFlex options is presented and the logistics of the overall course are reviewed. The challenges that were faced during course development and while offering the course, and how these were responded to, are discussed. Challenges with the rapid implementation of the HyFlex-based delivery model amidst the pandemic are reviewed. Additionally, differences between the San Francisco State University HyFlex model and the HyFlex-based model used in the course are discussed. Finally, plans for future offerings of this course are reviewed.

1. Introduction

This paper presents the efforts undertaken to develop and the implementation of a flexible learning defensive security course. The course covers the CompTIA Security+ requirements and is based on the HyFlex delivery model which was originally developed at San Francisco State University.

This paper discusses how a limited-flexibility model was transformed due to the COVID-19 pandemic into a highly flexible delivery model. Specifically, the course went beyond simply having lecture and laboratory components to offering a HyFlex Options Menu where students select between several options for each area of the class. Students were offered the opportunity to select between interactive lectures and reading, for presentation of the material. They were given the opportunity to take unit-specific quizlets and multi-unit spanning quizzes for testing. They were given the opportunity to choose between synchronous and asynchronous lab completion and given flexibility in their discussion board responses. Students were also given the opportunity to choose between an experiential immersion in industry experience, entrepreneurial experience and research experience.

The overall outline and instructional design of the course are presented. The implementation of each of the HyFlex options is presented and the logistics of the overall course are reviewed. The challenges that were faced during course development and while offering the course, and how these were responded to, are discussed.

Challenges with the rapid implementation of the HyFlex-based delivery model amidst the pandemic are reviewed. Additionally, differences between the San Francisco State University HyFlex model and the HyFlex-based model used in the course are discussed. Finally, plans for future offerings of this course are discussed.

2. Background

This section reviews prior work in two areas relevant to the course described in this paper. First, an overview of cybersecurity education is provided. Next, a discussion of the HyFlex educational model and its previous uses is presented.

2.1. Cybersecurity Education

Cybersecurity professionals are in high demand in the United States and worldwide, driving an urgent need for university graduates in this area [1]. In 2020, approximately a third of cybersecurity positions in the United States were vacant [2] and greater vacancy rates are projected in the future.

Given the significant need, a variety of techniques have been utilized in cybersecurity education to attempt to attract students and increase their interest, course satisfaction and retention. Cybersecurity education techniques have included puzzles [3] and challenges [4] as well as undergraduate research activities [5]. Other studies have assessed the use of techniques such as peer mentoring [6], peer instruction [7], games [8] and competitions [9] in cybersecurity education.

Some of these techniques work well in both online and in-person environments. Others depend on access to laboratory equipment or other facilities or are designed for interactions that are, at present, difficult to accomplish online. The COVID-19 pandemic drove an immediate need for institutions to provide effective cybersecurity education online.

2.2. HyFlex Course Design

A significant amount of prior work has been performed related to the development of the HyFlex course delivery model. The model has been demonstrated for undergraduate [10], graduate [11] and adult learning [12] courses across numerous disciplines ranging from teacher education [10], [13] to social work [14] to statistics [15].

The HyFlex model, according to Beatty, gives students “full control over their decisions to participate online or in the classroom” allowing them to balance their educational needs with other aspects of their life [16]. This is not without potential difficulties as Lakhal, Khechine and Pascot [17] found significant differences between student satisfaction and grades between students participating via different modes. Despite this, Rhoads [18] suggests that the HyFlex model can concurrently increase instructional efficiency along with satisfaction and student partipation flexibility. Heilporn and Lakhal [19], further, discuss how HyFlex courses can be used to drive student engagement, though Binnewies and Wang [20] raise engagement concerns, as well as concerns of course equity. Miller, Risser and Griffiths [21] discuss how the model can increase flexibility for instructors, as well.

Notably, innovation in HyFlex education is occurring in multiple areas. Leijon and Lundgren [22] have performed work on interconnecting between the physical course instruction location and “virtual spaces” to focus in creating interaction opportunities between students and the instructor. Keiper, et al. [23] have experimented with HyFlex integration of the pre-existing FlipGrid. Beatty [24] has proposed the use of HyFlex as a transitional approach to fully online instruction. An urgent need for flexibility and transition capability was created by the COVID-19 pandemic [25], though many universities were moving towards offering partially or fully online programs prior to the pandemic.

Several studies have assessed the HyFlex model, Kyei-Blankson [26] studied HyFlex learning outcomes, while Liu and Rodriguez [27] studied its impact more broadly. Rhoads [28] compared student learning outcomes and satisfaction levels for HyFlex and classroom-based course. Koskinen [29] and Wright [30] studied the model's utility in adult education courses and its ability to meet student needs.

3. Prior Design Approach of Undergraduate and Combined Undergraduate / Graduate Courses

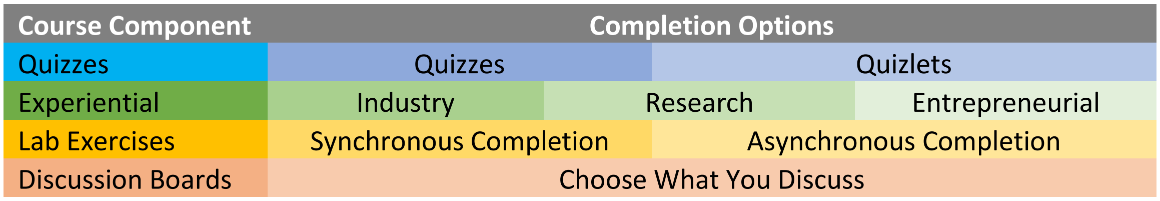
Prior to the COVID-19 pandemic, cybersecurity courses at North Dakota State University (NDSU) typically were either in-person courses, in-person flipped classroom courses or hybrid courses where distance students could connect in synchronously or watch videos of course lectures. A previous department chair had advocated a design once-and-reuse model where facilitators could run courses on a recurrent basis, after they had been designed by a faculty member, which led to some of these design decisions. Most undergraduate courses included both a lecture and lab component, with some using online labs and other courses using physical hardware.

4. HyFlex Course Design Overview

In response to the pandemic, NDSU implemented campus-wide use of the HyFlex model (excepting courses and departments with special equipment or accreditation requirements); however, exactly what HyFlex meant or required during this period of rapid change was unclear. In many cases, minimal NDSU HyFlex implementations meant only that a course was concurrently viewable from both an on-campus location and online.

For the defensive security course design, the instructor adapted the model proposed by Beatty [16] and sought to introduce flexibility in to each area of the course. The HyFlex Menu, presented in Figure 1, was used to present these options to students in the course.

The course ran during a standard 16-week (plus one week for finals) NDSU semester during the Spring of 2020. It used the textbook *CompTIA Security+ Guide to Network Security Fundamentals, 6th Edition* from Cengage.



Course Component	Completion Options		
Quizzes	Quizzes	Quizlets	
Experiential	Industry	Research	Entrepreneurial
Lab Exercises	Synchronous Completion	Asynchronous Completion	
Discussion Boards	Choose What You Discuss		

Figure 1. HyFlex Options Menu Used for the Course.

Notably, each key area of the course had multiple options for participation. These areas are discussed in Sections 5 through 9.

5. Content Presentation

Content presentation took two forms: lectures and textbook readings. Care was taken to make sure that all materials required for the quizzes or quizlets were covered in both areas so that students could choose between the two (and switch from week to week, if desired). In cases where lectures covered material that was not included in the book or included a demonstration, these lectures were recorded and made available online (and automatic transcriptions were available, if desired by students). Added content included a discussion of current cybersecurity trends and voting security. The latter included a demonstration of physical and electronic security vulnerabilities of a voting machine, which the instructor disassembled and highlighted vulnerabilities with during a class session.

6. Quizzes and Quizlets

To facilitate student flexibility in studying, students had the option to take quizzes or quizlets on the course content. Quizlets were short quiz-parts which could be taken on a unit-by-unit basis, while quizzes covered several units. Students, thus, had the flexibility to take the quizlets right after they read chapters (or attended relevant lectures), to take the quizlets on a unit-by-unit basis after several units or to take the quiz all-at-once. The corresponding quizzes and quizlets were due at the same time. The primary goal of the quizzes and quizlets was to encourage students to study the course materials and to demonstrate their understanding of them through application.

7. Lab Exercises

Lab exercises focused on the application of course materials. Lab exercises were offered online in a hosted environment and could be completed synchronously or asynchronously. Most students chose to complete the labs on their own and at their own pace, in most cases.

8. Discussion Boards

Discussion boards provided students an opportunity to explore technical concepts, cybersecurity impact and the implications of insecurity. In all cases, students were presented multiple articles to choose from. Students selected an article to read and briefly summarized it. They then were typically asked to comment on its importance and respond to the posts of two other students.

> This discussion board will focus on [topic], building on what we've learned during unit [#]. Please read one of the below articles and post a brief summary of what you've learned and why it is important (i.e., the societal, security or other implications) on the discussion board. Then, please reply to two others' posts.
>
> Please make your primary post by this next Wednesday [] and two response posts by the following Monday [].

Figure 1. Standard Discussion Board Assignment Format.

The standardized discussion board assignment format is presented in Figure 1. Table 1 lists two non-standard format discussion board assignments as well as the focus topics for all other weeks. Tables 2 to 12 present the articles that students were given to choose from (slight updates have been made to some tables in preparation for the next offering of the course). Notably, some of these discussion boards were not used in the Spring 2020 offering, to attempt to reduce student workload amidst the stresses of the pandemic.

Table 1. Discussion Board Assignments.

Topic	Discussion Board Assignment
1	For this week's discussion board, we'll be reviewing a number of different articles about cybersecurity, generally. Please read one of the below articles or one of the news articles in the news area of the discussion board. For the article that you read, please post a brief summary and then discuss the societal and/or security implications of the topic of the article. Please make one primary post by this upcoming Saturday [] and two response posts by the following Monday [].
2	For our second discussion board, we'll focus on what we can learn from reading cybersecurity news articles. Because of the rapidly changing nature of the field, cybersecurity professionals need to keep up to date with the latest security technologies, attacks, vulnerabilities and defenses. Please find a news article (some examples can be found in the cybersecurity news discussion board) that relates to malware or social engineering. This could be an article about an attack, a technical innovation or something else related to this topic. Please describe what is discussed in the article and what you learned from reading it. Both Google and Bing have news search engines that can help you find a news article. Ideally, try for one that is less than two months old. Please make one primary post by this upcoming Saturday [] and two response posts by the following Monday []. Also, please post a link to your news item to the news discussion board!
3	Standard format – cryptography focus
4/5	Standard format – cyberattacks focus
6	Standard format – device security focus
7	Standard format – wireless security focus
8	Standard format – mobile and embedded device security focus
9	Standard format – authentication focus
10	Standard format – vulnerability assessment focus
11	Standard format – business continuity focus
12	Standard format – cyber risks focus
13	Standard format – cyberattacks, impact and response focus

Table 2. Articles for Discussion Board Topic 1 – General.

Article	URL

Forno - Equifax breach is a reminder of society’s larger cybersecurity problems	https://theconversation.com/equifax-breach-is-a-reminder-of-societys-larger-cybersecurity-problems-84034
Kshetri - Why the IRS was just hacked – again – and what the feds can do about it	https://theconversation.com/why-the-irs-was-just-hacked-again-and-what-the-feds-can-do-about-it-54524
Forno - Overcoming ‘cyber-fatigue’ requires users to step up for security	https://theconversation.com/overcoming-cyber-fatigue-requires-users-to-step-up-for-security-70621
Akoto - Hackers could shut down satellites – or turn them into weapons	https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932
Graham - The difference between cybersecurity and cybercrime, and why it matters	https://theconversation.com/the-difference-between-cybersecurity-and-cybercrime-and-why-it-matters-85654
Shackelford - 30 years ago, the world’s first cyberattack set the stage for modern cybersecurity challenges	https://theconversation.com/30-years-ago-the-worlds-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges-105449

Table 3. Articles for Discussion Board Topic 3 – Cryptography.

Article	URL
Denning - Is quantum computing a cybersecurity threat?	https://theconversation.com/is-quantum-computing-a-cybersecurity-threat-107411
Kak - A quantum computing future is unlikely, due to random hardware errors	https://theconversation.com/a-quantum-computing-future-is-unlikely-due-to-random-hardware-errors-126503
Zuckerman & Chattopadhyay - How random is your randomness, and why does it matter?	https://theconversation.com/how-random-is-your-randomness-and-why-does-it-matter-59958
Buchanan - Bypassing encryption: ‘Lawful hacking’ is the next frontier of law enforcement technology	https://theconversation.com/bypassing-encryption-lawful-hacking-is-the-next-frontier-of-law-enforcement-technology-74122
Martin - Could encryption ‘backdoors’ safeguard privacy and fight terror online?	https://theconversation.com/could-encryption-backdoors-safeguard-privacy-and-fight-terror-online-53419
Steinfeld - Encryption today: how safe is it really?	https://theconversation.com/encryption-today-how-safe-is-it-really-37806

Table 4. Articles for Discussion Board Topic 4/5 – Cyberattacks.

Article	URL
Kshetri - After the NSA hack: Cybersecurity in an even more vulnerable world	https://theconversation.com/after-the-nsa-hack-cybersecurity-in-an-even-more-vulnerable-world-64090
Dean - ‘Zero-day’ stockpiling puts us all at risk	https://theconversation.com/zero-day-stockpiling-puts-us-all-at-risk-45637

McElfresh - Cyberattack on Ukraine grid: here’s how it worked and perhaps why it was done	https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802
McElfresh - Can the power grid survive a cyberattack?	https://theconversation.com/can-the-power-grid-survive-a-cyberattack-42295
Forno - How vulnerable to hacking is the US election cyber infrastructure?	https://theconversation.com/how-vulnerable-to-hacking-is-the-us-election-cyber-infrastructure-63241

Table 5. Articles for Discussion Board Topic 6 – Device Security.

Article	URL
Khan & Vallina-Rodriguez - Is your VPN secure?	https://theconversation.com/is-your-vpn-secure-109130
Fernandes - Security risks in the age of smart homes	https://theconversation.com/security-risks-in-the-age-of-smart-homes-58756
Fletcher - Hacked webcam site is another reminder to improve security online	https://theconversation.com/hacked-webcam-site-is-another-reminder-to-improve-security-online-34626
Hamlyn-Harris - Three reasons why pacemakers are vulnerable to hacking	https://theconversation.com/three-reasons-why-pacemakers-are-vulnerable-to-hacking-83362

Table 6. Articles for Discussion Board Topic 7 – Wireless Security.

Article	URL
Gregory - Wardriving and surviving: who else is using your Wi-Fi?	https://theconversation.com/wardriving-and-surviving-who-else-is-using-your-wi-fi-6009
Glance - Wi-Fi can be KRACK-ed. Here’s what to do next	https://theconversation.com/wi-fi-can-be-krack-ed-heres-what-to-do-next-85746
Woodward - The real phone hacking scandal is in your pocket	https://theconversation.com/the-real-phone-hacking-scandal-is-in-your-pocket-14245
Chen & Mao - Connected cars can lie, posing a new threat to smart cities	https://theconversation.com/connected-cars-can-lie-posing-a-new-threat-to-smart-cities-95339

Table 7. Articles for Discussion Board Topic 8 – Mobile & Embedded Device Security.

Article	URL
Vishwanath - Is the new iPhone designed for cybersafety?	https://theconversation.com/is-the-new-iphone-designed-for-cybersafety-83863
Kshetri - Using blockchain to secure the ‘internet of things’	https://theconversation.com/using-blockchain-to-secure-the-internet-of-things-90002
Harry - The quiet threat inside ‘internet of things’ devices	https://theconversation.com/the-quiet-threat-inside-internet-of-things-devices-109391
Oluwafemi - Can a hacker stop your car or your heart? Security and the Internet of Things	https://theconversation.com/can-a-hacker-stop-your-car-or-your-heart-security-and-the-internet-of-things-33273

Landau - Encrypted smartphones secure your identity, not just your data	https://theconversation.com/encrypted-smartphones-secure-your-identity-not-just-your-data-91715
Vallina-Rodriguez & Sundaresan - 7 in 10 smartphone apps share your data with third-party services	https://theconversation.com/7-in-10-smartphone-apps-share-your-data-with-third-party-services-72404

Table 8. Articles for Discussion Board Topic 9 – Authentication.

Article	URL
Warkentin, Renaud & Otondo - A secure relationship with passwords means not being attached to how you pick them	https://theconversation.com/a-secure-relationship-with-passwords-means-not-being-attached-to-how-you-pick-them-110557
Squire - Why we should not know our own passwords	https://theconversation.com/why-we-should-not-know-our-own-passwords-73747
Cranor, et al. - Choose better passwords with the help of science	https://theconversation.com/choose-better-passwords-with-the-help-of-science-82361
Lindqvist - Could a doodle replace your password?	https://theconversation.com/could-a-doodle-replace-your-password-56792
Lennon - The long history, and short future, of the password	https://theconversation.com/the-long-history-and-short-future-of-the-password-76690
Xu, Lin & Jin - My thoughts are my password, because my brain reactions are unique	https://theconversation.com/my-thoughts-are-my-password-because-my-brain-reactions-are-unique-98691
Ryoo - The age of hacking brings a return to the physical key	https://theconversation.com/the-age-of-hacking-brings-a-return-to-the-physical-key-73094

Table 9. Articles for Discussion Board Topic 10 – Vulnerability Assessment.

Article	URL
Holt - What are software vulnerabilities, and why are there so many of them?	https://theconversation.com/what-are-software-vulnerabilities-and-why-are-there-so-many-of-them-77930
Summers - Hunting hackers: An ethical hacker explains how to track down the bad guys	https://theconversation.com/hunting-hackers-an-ethical-hacker-explains-how-to-track-down-the-bad-guys-70927
Schmidt & White - Why don’t big companies keep their computer systems up-to-date?	https://theconversation.com/why-dont-big-companies-keep-their-computer-systems-up-to-date-84250
Shakarian - The Sunburst hack was massive and devastating – 5 observations from a cybersecurity expert	https://theconversation.com/the-sunburst-hack-was-massive-and-devastating-5-observations-from-a-cybersecurity-expert-152444
Forno - How vulnerable to hacking is the US election cyber infrastructure?	https://theconversation.com/how-vulnerable-to-hacking-is-the-us-election-cyber-infrastructure-63241

Levy - Companies should be on the hunt for gremlins in the open-source machine	https://theconversation.com/companies-should-be-on-the-hunt-for-gremlins-in-the-open-source-machine-41878

Table 10. Articles for Discussion Board Topic 11 – Business Continuity.

Article	URL
Shanapinda - Protecting our digital heritage in the age of cyber threats	https://theconversation.com/protecting-our-digital-heritage-in-the-age-of-cyber-threats-108252
Saebeler & Govindarasu - Electricity grid cybersecurity will be expensive – who will pay, and how much?	https://theconversation.com/electricity-grid-cybersecurity-will-be-expensive-who-will-pay-and-how-much-114137
Debar - Cybersecurity: high costs for companies	https://theconversation.com/cybersecurity-high-costs-for-companies-110807
Kshetri - As digital threats grow, will cyber insurance take off?	https://theconversation.com/as-digital-threats-grow-will-cyber-insurance-take-off-104371
Boiten & Wall - WannaCry report shows NHS chiefs knew of security danger, but management took no action	https://theconversation.com/wannacry-report-shows-nhs-chiefs-knew-of-security-danger-but-management-took-no-action-86501
Lemnitzer - Ransomware gangs are running riot – paying them off doesn't help	https://theconversation.com/ransomware-gangs-are-running-riot-paying-them-off-doesnt-help-155254
Parent - With the increase in remote work, businesses need to protect themselves against cyberattacks	https://theconversation.com/with-the-increase-in-remote-work-businesses-need-to-protect-themselves-against-cyberattacks-138255
Dupuy - CFO survey: firms being hacked, taking action to protect data	https://theconversation.com/cfo-survey-firms-being-hacked-taking-action-to-protect-data-99522

Table 11. Articles for Discussion Board Topic 12 – Cyber Risks.

Article	URL
Shackelford - How companies can stay ahead of the cybersecurity curve	https://theconversation.com/how-companies-can-stay-ahead-of-the-cybersecurity-curve-74414
Jalali - Defending hospitals against life-threatening cyberattacks	https://theconversation.com/defending-hospitals-against-life-threatening-cyberattacks-93052
Dean - Hard Evidence: how much is cybercrime really costing us?	https://theconversation.com/hard-evidence-how-much-is-cybercrime-really-costing-us-34473
Dolliver - After a data breach, it's consumers left holding the bag	https://theconversation.com/after-a-data-breach-its-consumers-left-holding-the-bag-33067
Vishwanath - Cybersecurity's weakest link: humans	https://theconversation.com/cybersecuritys-weakest-link-humans-57455

Baylon & Insua - Cybersecurity risks and how to manage them	https://theconversation.com/cybersecurity-risks-and-how-to-manage-them-154145

Table 12. Articles for Discussion Board Topic 13 – Cyberattacks, Impact and Response.

Article	URL
Csallner - Inside the fight against malware attacks	https://theconversation.com/inside-the-fight-against-malware-attacks-81433
Graham - MalwareTech's arrest sheds light on the complex culture of the hacking world	https://theconversation.com/malwaretechs-arrest-sheds-light-on-the-complex-culture-of-the-hacking-world-82136
Kshetri - Ransomware criminals are targeting US universities	https://theconversation.com/ransomware-criminals-are-targeting-us-universities-141932
Krapp - Penn State hack exposes theft risk of student personal data	https://theconversation.com/penn-state-hack-exposes-theft-risk-of-student-personal-data-42105
Denning - Cybersecurity's next phase: Cyber-deterrence	https://theconversation.com/cybersecuritys-next-phase-cyber-deterrence-67090
Govindarasu & Hahn - Cybersecurity of the power grid: A growing challenge	https://theconversation.com/cybersecurity-of-the-power-grid-a-growing-challenge-73102
Kharraz - It's easier to defend against ransomware than you might think	https://theconversation.com/its-easier-to-defend-against-ransomware-than-you-might-think-57258

As is clear from the tables, the discussion board topics spanned across numerous areas of cybersecurity. They provided students with an opportunity to learn about, discuss and apply technical concepts as well as critical concepts related to societal implications and risk assessment and management.

9. Immersion Experience

The immersion experience was a key feature of this offering of this course. Students were given three immersion options: industry, research or entrepreneurial. Students divided into groups based upon the immersion option that they wanted to pursue as well as the topics that they indicated interest in. Several project topics were suggested for each category and student groups were free to propose their own.

In the industry option, one group of students had an opportunity to explore the NDSU network and its security. A second group helped a local business (which one of the students was working at) to design a security testing exercise which was deployed by the company's staff who reported back (somewhat abstracted, for security purposes, results to the students). In both cases, the groups made contacts with working IT professionals.

In the entrepreneurial option, students could propose a business concept or technology that they wanted to focus on. Business concepts could be either entrepreneurial (new business) or intrepreneurial (startup within an existing company). Concepts related to the development of a web-based training tool and a mobile application were proposed and developed by student teams.

Finally, in the research option, student groups got to participate in small components of bona fide research projects. One group worked on extending a facial feature steganography technique that was previously proposed by Marella, Straub and Bernard [31]. A second group worked on creating a user interface for cybersecurity command decision making while a third group looked into deceptive content identification, based on prior work [32]–[34]. It is likely that at least one of the research option groups will end up publishing a conference paper on their work.

This was the first implementation of this choice-of-immersion concept. The further development of this is a key area of future work.

10. COVID-19 Pandemic Logistics

While this course was deigned with the educational response to the COVID-19 pandemic in mind, the pandemic never-the-less created some logistical issues for the course. First, delays in the receipt of video conferencing equipment resulted in the remote synchronous participation capability not being fully available in the room until two-thirds of the way through the semester. In response to this issue, a portable distance studio was developed for use in this course. This kit could be quickly setup be the instructor before the class and rapidly disassembled after the class. This allowed the instructor to provide remote synchronous participation capabilities while these were not available in most other classes due to similar equipment receipt and installation delays.

Second, the immersion experiences were made far more challenging by the pandemic. The development of these experiences was already planned; however, the pandemic introduced the logistical challenge of connecting students between on- and off-campus locations as well as those that the students had to interact with. For the group exploring the security of the NDSU network, privacy concerns necessitated that much of the work be done physically on campus.

Third, the general level of student pandemic fatigue required some workload reductions (principally in reducing discussion boards and de-scoping some projects) to facilitate students' successful completion.

Finally, several activities that could have been more hands-on, such as the opportunity for students to examine the components of the disassembled voting machine, were not available due to many students participating at a distance and the potential disease transmission risks of multiple individuals handling hardware. While the model developed for this course will likely be used in the future, several enhancements will be easily incorporated when these limitations are no longer present, post-pandemic.

11. Conclusions and Future Work

This paper has presented the development of a new defensive security course and its implementation using the HyFlex model. It has introduced the concept of the HyFlex Menu, to show students their options for participation in each area. Further, it has briefly presented the initial work in course-based immersion modules, which are a key are for future development and study, as they appear poised to provide significant benefits for students.

In addition to additional ongoing work on the development of course-based immersion modules, another key area of work, post-pandemic, will be the comparison of different HyFlex model course designs to on campus and pure distance equivalents. While HyFlex courses clearly offer students flexibility, the exact tradeoffs posed are unclear from the literature. This particular course's implementation suggests that some trade-offs exist, particularly in the areas of the immersion modules and hands-on laboratory experiments. However, once pandemic safety concerns are no longer present, limited on-campus participation requirement strategies may be an effective approach to allow much of this flexibility while minimizing the limitations of the HyFlex model. Further assessment of these trade-offs and loss minimization is planned in the future.

Acknowledgement

The development of student immersive experiences was partially supported by the NDSU Challey Institute for Global Innovation and Growth.

References

[1] K. Evans and F. Reeder, *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters*. Washington, DC: Center for Strategic & International Studies, 2010.

[2] Cyber Seek, "Cybersecurity Supply/Demand Heat Map," *Cyber Seek Website*, 2019. https://www.cyberseek.org/heatmap.html (accessed Feb. 03, 2019).

[3] D. Dasgupta, D. M. Ferebee, and Z. Michalewicz, "Applying Puzzle-Based Learning to Cyber-Security Education," in *Proceedings of the 2013 on InfoSecCD '13 Information Security Curriculum Development Conference - InfoSecCD '13*, 2013, pp. 20–26, doi: 10.1145/2528908.2528910.

[4] R. S. Cheung, J. P. Cohen, H. Z. Lo, and F. Elia, "Challenge Based Learning in Cybersecurity Education," 2011, Accessed: Sep. 23, 2018. [Online]. Available: https://search.proquest.com/docview/1272087912?pq-origsite=gscholar.

[5] C. Frank, J. McGuffee, and C. Thomas, "Early undergraduate cybersecurity research," *J. Comput. Sci. Coll.*, vol. 32, no. 1, pp. 46–51, 2016, Accessed: Sep. 23, 2018. [Online]. Available: https://dl.acm.org/citation.cfm?id=3007235.

[6] V. P. Janeja, C. Seaman, K. Kephart, A. Gangopadhyay, and A. Everhart, "Cybersecurity workforce development: A peer mentoring approach," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, Sep. 2016, pp. 267–272, doi: 10.1109/ISI.2016.7745487.

[7] P. Deshpande, C. B. Lee, and I. Ahmed, "Evaluation of Peer Instruction for Cybersecurity Education," 2019, doi: 10.1145/3287324.3287403.

[8] A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen, "Exploring game design for cybersecurity training," in *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, May 2012, pp. 256–262, doi: 10.1109/CYBER.2012.6392562.

[9] R. S. Cheung, J. P. Cohen, H. Z. Lo, F. Elia, and V. Carrillo-Marquez, "Effectiveness of

Cybersecurity Competitions," 2012, Accessed: Feb. 03, 2019. [Online]. Available: https://search.proquest.com/docview/1426803138?pq-origsite=gscholar.

[10] D. Carbonara, "Teaching STEM to Pre-Service, PK-4 Student-Teachers Using HyFlex Student...," in *SITE Interactive Conference*, Oct. 2020, vol. 2020, no. 1, pp. 330–333.

[11] M. M. M. Abdelmalak and J. L. Parra, "Expanding Learning Opportunities for Graduate Students with HyFlex Course Design," *Int. J. Online Pedagog. Course Des.*, vol. 6, no. 4, 2016.

[12] M. Abdelmalak, "Towards Flexible Learning for Adult Students: HyFlex Design," in *Society for Information Technology & Teacher Education International Conference*, Mar. 2014, vol. 2014, no. 1, pp. 706–712.

[13] A. Raes, M. Pieters, and P. Bonte, "Hyflex Learning within the Master of Teaching Program@KU Leuven," in *Hybrid-Flexible Course Design*, 1st ed., B. J. Beatty, Ed. Provo, UT: EdTech Books, 2019.

[14] B. R. Malczyk, "Introducing Social Work to HyFlex Blended Learning: A Student-centered Approach," *J. Teach. Soc. Work*, vol. 39, no. 4–5, pp. 414–428, Oct. 2019, doi: 10.1080/08841233.2019.1652226.

[15] J. B. Miller and M. E. Baham, "Comparing the HyFlex (hybrid-flexible) model of course delivery in an introductory statistics course and a probability and statistics course for engineers and scientists," 2018.

[16] B. J. Beatty, "Teaching a Hybrid-Flexible Course," in *Hybrid-Flexible Course Design*, 1st ed., B. J. Beatty, Ed. Provo, UT: EdTech Books, 2019.

[17] S. Lakhal, H. Khechine, and D. Pascot, "Academic Students' Satisfaction and Learning Outcomes in a HyFlex Course: Do ...," in *E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education*, Oct. 2014, vol. 2014, no. 1, pp. 1075–1083.

[18] D. Rhoads, "Increasing Flexibility, Satisfaction, and Efficiency Using the Hybrid Flexible Approach," in *Hybrid-Flexible Course Design*, 1st ed., B. J. Beatty, Ed. Provo, UT: EdTech Books, 2019.

[19] G. Heilporn and S. Lakhal, "Converting a graduate-level course into a HyFlex modality: What are effective engagement strategies?," *Int. J. Manag. Educ.*, vol. 19, no. 1, p. 100454, Mar. 2021, doi: 10.1016/j.ijme.2021.100454.

[20] S. Binnewies and Z. Wang, "Challenges of Student Equity and Engagement in a HyFlex Course," in *Blended Learning Designs in STEM Higher Education*, Springer Singapore, 2019, pp. 209–230.

[21] J. Miller, M. Risser, and R. Griffiths, "Student Choice, Instructor Flexibility: Moving Beyond the Blended...," *Issues Trends Educ. Technol.*, vol. 1, no. 1, pp. 8–24, 2013.

[22] M. Leijon and B. Lundgren, "Connecting physical and virtual spaces in a HyFlex pedagogic model with a focus on teacher interaction," *J. Learn. Spaces*, vol. 8, no. 1, 2019, Accessed: Mar. 10, 2021. [Online]. Available: http://ls00012.mah.se/handle/2043/29362.

[23] M. C. Keiper, A. White, C. D. Carlson, and J. M. Lupinek, "Student perceptions on the benefits of Flipgrid in a HyFlex learning environment," *J. Educ. Bus.*, pp. 1–9, Oct. 2020, doi: 10.1080/08832323.2020.1832431.

[24] B. Beatty, "Transitioning to an Online World: Using HyFlex Courses to Bridge the Gap," in *EdMedia + Innovate Learning*, Jun. 2007, pp. 2701–2706.

[25] A. N. Miller, D. D. Sellnow, and M. G. Strawser, "Pandemic pedagogy challenges and

opportunities: instruction communication in remote, HyFlex, and BlendFlex courses," *Commun. Educ.*, 2020, doi: 10.1080/03634523.2020.1857418.

[26] L. Kyei-Blankson and F. Godwyll, "An Examination of Learning Outcomes in Hyflex Learning Environments," in *E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education*, Oct. 2010, vol. 2010, no. 1, pp. 532–535.

[27] C. Y. A. Liu and R. C. Rodriguez, "Evaluation of the impact of the Hyflex learning model," *Int. J. Innov. Learn.*, vol. 25, no. 4, pp. 393–411, 2019, doi: 10.1504/IJIL.2019.099986.

[28] D. D. Rhoads, "Traditional, Online or Both? A Comparative Study of University Student Learning and Satisfaction Between Traditional and Hyflex Delivery Modalities," Concordia University, Irvine, CA, 2020.

[29] M. Koskinen, "Understanding the Needs of Adult Graduate Students: An Exploratory Case Study of a HyFlex Learning Environment," Northeastern University, 2018.

[30] D. Wright, "The HyFlex course design: A case study on adult and career education courses," *Natl. Soc. Sci. J.*, vol. 48, no. 2, pp. 88–93, 2016.

[31] P. Marella, J. Straub, and B. Bernard, "Development of a facial feature based image steganography technology," in *Proceedings of the 6th Annual Conference on Computational Science and Computational Intelligence*, Dec. 2019, pp. 675–678, doi: 10.1109/CSCI49370.2019.00126.

[32] N. Snell, W. Fleck, T. Traylor, and J. Straub, "Manually classified real and fake news articles," in *Proceedings - 6th Annual Conference on Computational Science and Computational Intelligence, CSCI 2019*, Dec. 2019, pp. 1405–1407, doi: 10.1109/CSCI49370.2019.00262.

[33] B. Kalvoda, B. Stoick, N. Snell, and J. Straub, "Evaluation of Algorithms for Fake News Identification," 2019.

[34] B. Stoick, N. Snell, and J. Straub, "Fake news identification: A comparison of parts-of-speech and N-grams with neural networks," in *Proceedings of SPIE - The International Society for Optical Engineering*, 2019, vol. 10989, doi: 10.1117/12.2521250.