Journal of Cybersecurity Education, Research and Practice

Volume 2020 | Number 2 Article 4

January 2021

Applying High Impact Practices in an Interdisciplinary Cybersecurity Program

Brian K. Payne
Old Dominion University, bpayne@odu.edu

Lisa Mayes
Old Dominion University, lmayes@odu.edu

Tisha Paredes
Old Dominion University, tparedes@odu.edu

Elizabeth Smith
Old Dominion University, exsmith@odu.edu

Hongyi Wu
Old Dominion University, h1wu@odu.edu

See next page for additional authors

Applying High Impact Practices in an Interdisciplinary Cybersecurity Program

Abstract

The Center for Cybersecurity Education and Research at Old Dominion University has expanded its use of high impact practices in the university's undergraduate cybersecurity degree program. Strategies developed to promote student learning included learning communities, undergraduate research, a robust internship program, service learning, and electronic portfolios. This paper reviews the literature on these practices, highlights the way that they were implemented in our cybersecurity program, and discusses some of the challenges encountered with each practice. Although the prior literature on high impact practices rarely touches on cybersecurity coursework, the robust evidence of the success of those practices provides a sound rationale for applying them across the curricula. Challenges confronted included developing partnerships, introducing students to new learning strategies, and gaining buy in from faculty. Despite these challenges, the authors' experiences with the efforts also support using high impact practices in cybersecurity programs. Recommendations for other cybersecurity programs seeking to expand the use of high impact practices include integrating experiential learning throughout the curricula, developing campus-wide partnerships, embracing the interdisciplinary nature of cybersecurity, demonstrating the purpose of the practices, providing faculty development, emphasizing writing, and embracing failure.

Keywords

cybersecurity, electronic portfolios, learning communities, internships, service learning, high impact practices

Cover Page Footnote

This research is supported in part by the National Science Foundation under grant DGE1723635 and the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation and workforce development. For more information about CCI, visit cyberinitiative.org."

Authors

Brian K. Payne, Lisa Mayes, Tisha Paredes, Elizabeth Smith, Hongyi Wu, and ChunSheng Xin

INTRODUCTION

Cybersecurity has grown tremendously as an academic area of study over the past decade. New academic majors and degree programs have been created to respond to the growing demand for a cybersecurity workforce with more than 500,000 job vacancies across the United States (Cyberseek.org, 2020). Few other academic programs have such a clear connection between career opportunities and the need for graduates. On the one hand, this high demand for cybersecurity graduates bodes well for cybersecurity students and educators. After all, cybersecurity is a field touting a "zero percent" unemployment rate (Morgan, 2016). On the other hand, with such high demand for cybersecurity workers, it is critical that cybersecurity education programs produce graduates who are actually able to do the work needed in those unfilled careers.

The challenge, then, is not simply about producing more graduates in cybersecurity. Instead, the real challenge is to produce more *qualified* graduates in cybersecurity. To do so, much of the scholarship on cybersecurity education has demonstrated the need to teach students certain knowledge, skills, and abilities that would ultimately translate into successful cybersecurity workers (Mirkovic & Benzel, 2012; Weiss et al., 2015). The mere application of these knowledge, skills, and abilities is not enough, however, to produce career-ready students. To be sure, it is necessary that students possess these qualities. But possessing these knowledge, skills, and abilities is not sufficient. Indeed, many studies show that cybersecurity graduates should possess the "softer" skills like communication skills, teamwork abilities, critical thinking skills, problem solving capabilities, skills related to transferring knowledge, and so on, as well as the traditional knowledge, skills, and abilities needed in these careers (Jones et al., 2018).

One question that arises is how to teach soft skills. The answer lies not in the specific material covered, but in the strategies used to cover the course material. In other words, it is not "*what" students are being taught*, but *"how" they are learning* that becomes important. Cybersecurity scholars have recognized "a need for instructional methods that engage students in reasoning about complex scenarios" (Thompson et al., 2019). Higher education experts point to the use of "high impact practices" as being particularly helpful in developing these all too important skills.

High impact practices are learning strategies that have been empirically shown to be successful in producing positive student learning outcomes (Eynon & Gambino, 2017; Kuh, 2008; Kuh et al., 2017). Moreover, these practices have been shown to be especially fruitful for disadvantaged populations (Conefrey, 2018; Finley, 2011). The American Association for Colleges and Universities has identified the following types of high impact practices: first-year seminars, common intellectual experiences, writing intensive courses, learning communities,

service learning, internships, undergraduate research, collaborative assignments, diversity/global learning, capstone projects, and electronic portfolios (Kuh, 2008).

With funding from the National Science Foundation (NSF), the authors integrated five of these high impact practices into the interdisciplinary cybersecurity undergraduate program at Old Dominion University (ODU). Specifically, the authors' efforts included developing learning communities, fostering undergraduate research projects, teaching select courses using service-learning activities, expanding internship opportunities, and connecting interdisciplinary courses through ePortfolios. These high impact practices were selected given the large body of research showing how these practices benefit both students and the community at large (Simons et al., 2020; Springer et al., 2019). In this paper, the literature surrounding each of these high impact practices is described along with the authors' experiences in integrating them into their curricula. Recommendations for other cybersecurity programs seeking to use similar high impact practices in their curriculum are offered.

RATIONALE FOR HIGH IMPACT PRACTICES IN CYBERSECURITY AND PROGRAM OVERVIEW

A number of studies have been conducted on the success of high impact practices in promoting student learning (Eynon & Gamble, 2017; Kilgo et al. 2015). These studies tend to focus on general student populations (Bonet & Waters, 2016; Brownell & Swaner, 2009), though some scholars have demonstrated how high impact practices can be used successfully with STEM majors (Harrington, & Luo, 2016; Porter, 2017). Table 1 summarizes the learning outcomes identified by the authors for each high impact practice in their cybersecurity program and the specific value of those practices for students and the community.

Briefly, when students engage in learning communities, they should learn more about their careers, gain stronger connections, and apply their knowledge in different settings (helping students to transition and improving their learning while providing more efficient use of academic credits). When students do internships, they should be able to apply their coursework to a work setting, enhance their communication skills, and demonstrate their abilities to be professionals (helping students gain careers and providing the workforce better prepared workers). Students doing undergraduate research will be able to explain how knowledge is created, design research products, and show how research is done the real-world settings (enhancing their critical thinking/writing skills and providing stronger workers for the workforce). Serving learning outcomes include preparing students so they are able to solve community problems and reflect on civic identity (enhancing student empathy while helping students and community members

learn). Finally, the learning outcomes of electronic portfolios include preparing students to digitally showcase their skills, engage in deeper learning, and connect their educational goals and personal experiences.

Table 1. Learning Outcomes and Value of HIPS to Students and the Community

	Learning Outcomes+, After finishing, student will be able to:	Benefits
Learning Communities	1 Demonstrate a deeper knowledge of potential careers in their major 2 Connect to university and peers through in and out-of-class experiences 3 Apply content knowledge across multiple settings	To students: Less isolation Better transition to college Improved learning
		To community: Higher graduation rates and less unused credits
Internships	1 Apply prior learning to work setting 2 Use communication strategies/skills appropriate to settings and audiences 3 Conduct themselves according to appropriate professional standards, customs, and practices in workplace	To students: Communication/teamwork Work experience
		To community: Skilled workforce Ongoing supply of labor
Undergraduate Research	1 Explain how knowledge is created and discovered 2 Design research, project that addresses problems in our community 3 Connect how research skills can be applied to real world settings	To students: Critical thinking/writing skills Research products created
		To community: Knowledge from the research Stronger pool of workers
Service Learning	1 Implement solutions to meet community needs 2 Reflect on sense of civic identity 3 Apply knowledge to identify social problems	To students: Communication/teamwork Empathy enhanced
		To community: Civic engagement Reciprocal learning
ePortfolios	1 Digitally showcase skills 2 Create digital resumes 3 Engage in deeper learning	To students: Deep learning Digital safety
		To community: Potential employees Learn from students

Perhaps due to the relative infancy of the cybersecurity discipline, few studies have explored the application of high impact practices in cybersecurity programming. After reviewing the literature on five impact practices, the authors describe the results of their efforts to integrate these high impact practices into their cybersecurity curriculum and provide recommendations for others considering the use of high impact practices in cybersecurity coursework.

Learning Communities and Cybersecurity

Learning communities are linked-courses designed to promote co-curricular connections between students and faculty members. While many different types of learning communities have been identified, the most common typology captures four types: curricular learning communities, classroom learning communities, residential learning communities (also known as living learning communities), and student-type learning communities (e.g., Women in STEM) (Lenning & Ebbers, 1999). A voluminous amount of literature has explored the success of learning communities (Andrade, 2007; Gebauer et al., 2020; Tinto, 1998). The value of learning communities in reducing student isolation (Johnson, 2000; Walton et al., 2019), promoting student learning (Lenning & Ebbers, 1999; Tinto, 2019), and enhancing retention and graduation rates (Dagley et al., 2016) has been well documented in the literature.

Learning communities have a long history in higher education. Some have suggested that early residential universities in the colonial days were designed, in many ways, within a learning community framework (Fink & Inkelas, 2015). The use of learning communities changed course in the 20th century. The modern version of learning communities is traced to calls from reformers who have been demanding over the past two decades that higher education institutions implement pedagogical strategies that more successfully promote student learning (Fink & Inkelas, 2015). Describing this re-emphasis on learning communities, one higher education expert points out, “At no time has it been more important to look carefully at what we do and be able to document its effectiveness” (Smith, 2001, p. 4).

The growth of learning communities did not occur equally across disciplines. As one author team notes, “Despite their long history, learning communities are not common in computing” (Settle & Steinbach, 2018, p. 167). This suggests that there is an opportunity to expand this high impact practice more broadly into computing majors, including cybersecurity.

Recognizing the value of learning communities, the cybersecurity team created freshmen learning communities, sophomore learning communities (SLC), and living learning communities for cybersecurity majors at Old Dominion University.

Incoming cybersecurity freshmen were offered the opportunity to enroll in the freshmen and living learning communities. Courses in the freshmen learning communities included Introduction to Criminology (CRJS 215S), Basic Information Literacy and Research, and Cyber Explorers and University Orientation (CYSE 100). Students enrolled in the living learning community lived on the same floor in a residential hall, with a cybersecurity lab added in the common area for the students. Those students enrolled in Cyber Explorers and University Orientation. The Sophomore Learning Community was offered to second year cybersecurity majors, with two connected courses: Cybersecurity Technology, and Society (CYSE 200T) and Interdisciplinary Theory and Concepts (IDS 300W). The authors initially planned on requiring S-STEM cybersecurity students to enroll in the sophomore learning community, but the course scheduling could not accommodate the various course schedules of the students.

Undergraduate Research and Cybersecurity

Undergraduate research was also integrated into the suite collection of high impact practices offered to our students. An abundance of evidence exists showing the significant value of undergraduate research across all academic disciplines. Cybersecurity is no different. One author team summed up the value of cybersecurity undergraduate research projects in this way: "The benefits of engaging [cybersecurity] students in discipline related research early in their undergraduate studies include: developing teamwork skills, improving creative problem-solving abilities, creating a better understanding of career options within computing, and fostering an enthusiasm for the subject material that should improve retention of computing major" (Frank et al., 2016, p. 46). The value of undergraduate research programming is clear, though it seems that such efforts are still underutilized in cybersecurity programs.

Our undergraduate research programming followed the same process other undergraduate research initiatives follow. A request for proposals was released and students were given the opportunity to propose research projects to be conducted over the semester. While students were asked to identify possible mentors, not all proposals included specific mentors. The undergraduate research program director worked with the students in those cases to identify possible mentors. Students were given a $2,000 stipend. ODU mentors were given a $1,150 stipend and external mentors were given a $1,250 stipend. In all, 16 students completed undergraduate research projects. The students investigated security issues on a broad range of topics, from Blockchain, drones, artificial intelligence, malware, LiDAR, RFID, smart weapons, social media, vulnerability management, user privacy, to cyber bullying. Each student submitted a project report and a poster after his/her project was completed.

While our undergraduate research efforts discussed here and supported by the NSF project focused on student/mentor research, it is important to recognize that, as others have demonstrated, research projects can be integrated even into the most basic, introductory cybersecurity courses (Dupuis, 2017). Such an approach provides a more cost-effective strategy to integrate cybersecurity research into undergraduate cybersecurity curricula.

Internships and Cybersecurity

Internships are perhaps the longstanding staple in the list of high impact practices. While some have lamented the lack of practical skills in some college graduates, cybersecurity internships provide students the opportunity to gain skills they would not gain from stand-alone traditional coursework experiences (Carlin & Manson, 2016; Crumpler & Lewis, 2019). One author puts it simply: "Internships ensure sure footing" (Fussell, 2002, p. 64). Another way to put it is that internships help to prepare students for their subsequent careers (McGettrick, 2013). Despite the overwhelming benefit of internships, many students may opt out of them. Reasons that computing majors have been found to not do internships include self-efficacy issues, application issues, and alternate priorities (Kapoor & Gardner-McCune, 2020).

One way to overcome these issues is to require students to do internships rather than to offer them as electives. A regional study of cybersecurity businesses showed the value that employers place on internships. As a result of that study, a decision was made in 2017 to require cybersecurity students to either do an internship or an "entrepreneurship". With funding from NSF, we were able to offer students stipends to do internships in businesses that were not able to pay the students. The internship course required students to write a research paper demonstrating how their coursework related to their internship experience. Students were required to work for 50 hours for each credit they were registered for in their registration. All of the students registered for 3 credit internships, requiring them to work 150 hours over the term.

Service Learning and Cybersecurity

National research shows that service learning is quite powerful regarding its potential impact on student learning (Eyler & Giles, 1999). This educational practice can be traced to the early sixties when a group of advocates and scholars called for the integration of classroom learning experiences and community service practices (Stanton et al., 1999). One service learning scholar provided an early definition of service learning, referring to the experience as "reciprocal learning" (Sigmon, 1979). The reciprocal nature means that students and partners should both benefit from the service learning experience (Furco, 1996). A typology

offered by Sigmon (1994) offers a simple way to understand what is meant by the phrase service learning (see Table 2). In pure "SERVICE LEARNING," according to Sigmon, "service" and "learning" are equally emphasized. Often times, either service or learning is over emphasized at the expense of the other. The ideal is to have both equally emphasized, which would mean both students and the community benefit from the service learning engagement.

Table 2. Service Learning Typology

	Service Emphasis	Learning Emphasis
Cybersecurity SERVICE Learning	Primary	Secondary
Cybersecurity Service LEARNING	Secondary	Primary
cybersecurity service learning	Separate from learning	Separate from service
CYBERSECURITY SERVICE LEARNING	Equal to Learning	Equal to Service

Source: Adapted from Sigmon, 1994

In many ways, the service learning revolution preceded the creation of the cybersecurity discipline. Yet, some computing professors were ahead of their time so to speak with the a3pplication of service learning in computer security courses. Dark (2004), for example, worked with her information technology and computer science students to have them develop risk assessments for local schools. As a result of the service learning experiences, students learned how to conduct information security risk assessments and develop recovery plans if information is breached.

More recently, a group of information assurance students worked with their institution's IT staff to do cybersecurity awareness trainings, with the project helping the students learn important communication skills while also promoting a safer cyber environment at the institution (Innocenzi, 2018). In another recent example, a group of students conducted penetration tests on a local company, at their request, to identify possible security weaknesses (Kirk et al., 2019). Students learned about social engineering and the company was able to gather useful information to improve its security.

Working with the Office of Service Learning and Civic Engagement, our faculty in six different courses developed service learning assignments in their cybersecurity courses. The assignments and courses included the following:

- Students enrolled in Cybersecurity Fundamentals (ECE 416) helped organize challenges for the region's Great Computer Challenge in Spring 2018.

- Students enrolled in Cybercrime and Cybersecurity (CRJS 405) created cybersecurity teaching aides and lesson plans for students and teachers from a local high school in summer 2018.
- In Fall 2018, students enrolled in an online Cyber Law (CYSE/CRJS 406) class developed information packets that could be used to teach young people about the importance of cyber privacy.
- In Fall 2018, a group of pre-service teacher education students worked with an education professor and cybersecurity faculty to develop programming, including games and information about games and career options, for fifth graders. The programming was delivered to a group of fifth graders by the pre-service teachers.
- In Summer 2019, students enrolled in Cybercrime and Cybersecurity (CRJS 405) identified their own service learning assignments and designed strategies to use their knowledge to address a social problem related to cybersecurity.
- In Spring 2020, students enrolled in Cybersecurity Techniques and Operations (CYSE 301) developed modules that were used in the ODU Math and Computing Festival. Facilitators from the challenge indicated they would continue to use the projects in future activities.

Electronic Portfolios and Cybersecurity

Electronic portfolios (ePortfolios) in their simplest form are extensions of the traditional printed portfolios students or department faculty used to maintain to help monitor student progress in courses or academic programs. Much more versatile than traditional printed portfolios, ePortfolios provide for deeper learning (Eynon & Gambino, 2017), the availability of rich assessment data (Bhattacharya & Hartnet, 2007), the ability to showcase learning (Cambridge, 2010), integrated learning (Bokser et al., 2016), and increased awareness about digital safety (Baris & Tosun, 2013). Regarding deeper learning, when compiling ePortfolios students are encouraged to engage in self-reflection and find meaning in the material they are learning about (Alexiou & Paraskeva, 2010). In terms of assessment data, the archiving of all student work electronically provides a great amount of student learning outcome assessment data (Buzzetto-More, 2010). Showcasing learning also becomes feasible through ePortfolios and this may help students find careers. Integrated learning occurs when students are shown how to use their ePortfolios to connect course material across multiple courses or between assignments within a single course or learning experience. Finally, increased digital literacies for students and recognition that students can control their digital identities result from the actual creation of a digital presence (Buyarski el al., 2015). This final point fits well with suggestions in the academic literature that cybersecurity students need to

be taught about social media risks and how their use of social media could have long-term consequences for their careers (Rivera et al., 2017).

These multiple benefits of electronic portfolios led the cybersecurity faculty to identify ways to expand the use of electronic portfolios in their program. Working with Old Dominion University's Center for High Impact Practices, the cybersecurity program integrated ePortfolio development into the curricula. The steps we followed included identifying courses that should be a part of the ePortfolio template, developing the ePortfolio template, training faculty how to use ePortfolios, implementing the ePortfolio program, assessing progress, and making changes to the process. The first step included detailed conversations between the faculty and staff from the ePortfolios and Digital Initiatives Office. As a result of those discussions, a decision was made to ask students to include materials from the following courses in their ePortfolios: CYSE 200T (Cybersecurity, Technology, and Society), CYSE 368 (Cybersecurity Internship), a cybersecurity law or ethics course, a cybersecurity foundations course, and a cybersecurity fundamentals course).

The second step included the development of a template that cybersecurity students could use to develop their ePortfolios. This step was carried out by the director of ePortfolios and Digital Initiatives with feedback from cybersecurity faculty. The template was created to help students develop their ePortfolios. Figure 1 shows a visual of the homepage for the template.

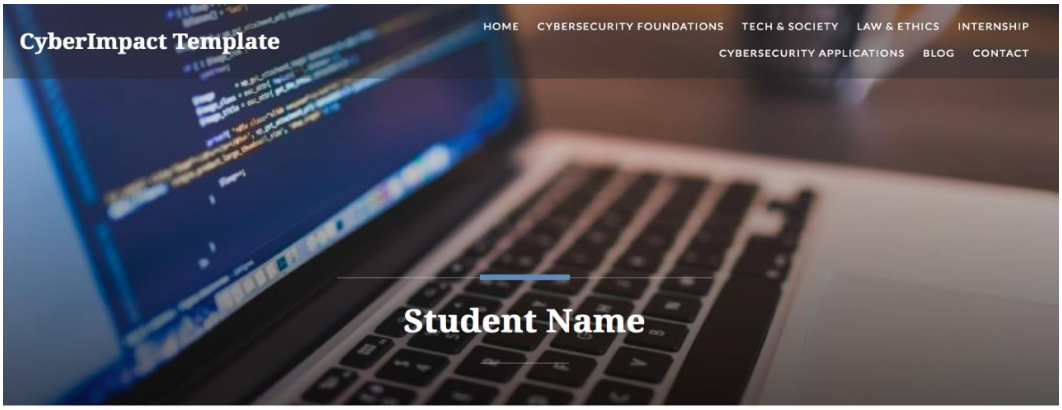

Figure 1. Cybersecurity ePortfolio template

The third step was training faculty how to use and integrate ePortfolios into their courses. The training was delivered by the director of the ePortfolio and Digital Initiatives unit. A recent English PhD with expertise in medieval literature, the

director was notably much more advanced than our cybersecurity faculty in talking about how to use digital technologies to help students learn. Remarkably, few of the cybersecurity faculty had previously been exposed to ePortfolios.

The fourth step, implementation, was not as seamless as expected. The obstacles and barriers became clear in our fifth step – assessment. Although the university provided a wide range of support, the interdisciplinary nature of our degree program made it harder to require faculty to include ePortfolios in their courses. In addition, students and faculty were often unable or unwilling to seek support that would help them in developing their ePortfolios.

The final step, making changes to the process, is ongoing. One change effort was a change in the courses to be included in the ePortfolio. In particular, a programmatic decision was made to have students include work from cybersecurity courses that were specifically under the control of the cybersecurity program. In doing so, the problems we faced as an interdisciplinary program were eliminated. Students are still able to include computer engineering, computer science, criminal justice, philosophy, and information technology courses in the portfolios, but there is no expectation or requirement that those courses be included. Another change was the creation of training videos to help faculty and students better understand the ePortfolio process.

PROGRAM ASSESSMENT RESULTS

Others have shown how case studies are effective tools to teach about cybersecurity (Cai & Arney, 2018). Case studies can also serve as a tool for empirically assessing the success of those teaching strategies. With this in mind, the high impact practices were assessed through a case study framework. Methods used included reviewing available student success data, surveying students who completed different high impact practices, reviewing materials submitted by students in different high impact practices, and reviewing "what worked" and "didn't work" for each high impact practice. After reviewing the findings from these different assessment processes, implications based on the authors' experiences and the results of the assessment are provided.

Learning Communities Assessment

Table 3 shows the retention and grade point average of the students enrolled in cybersecurity learning communities. As shown in the table, there are mixed results, especially with the lower retention rate of the Fall 2018 freshman learning community. The overall success of the communities, however, is notable. For example, the higher grade point averages of learning community students (excluding living learning communities) over all other freshman is noteworthy. It

is not clear why the living learning community cohort had a lower grade point average in Fall 2019, though the authors believe this year was an anomaly given the success of those students in prior years. In addition, a survey of 16 cybersecurity learning community freshmen found that: 88% of students agreed that because of the ILC experience, they would recommend Impact Learning Communities to a friend, and 82% agreed they made at least one friend that they will stay in touch with after the semester. Even stronger support for learning communities was found in a survey of Fall 2018 learning community participants, albeit with a much smaller sample (n=5).

Table 3. Cybersecurity Impact Learning Communities (ILCs) & Living-Learning Communities Fall 2017, Fall 2018, & Fall 2019, Grade Point Averages for Cybersecurity Communities & All First-Year Students

Cohort*	Fall 19 GPA	Fall 18 GPA	Fall 17 GPA
Freshmen Cybersecurity LC	3.14 (n=21)	2.81 (n=24)	2.69 (n=26)
Sophomore Cybersecurity LC+	3.29 (n=20)	-	-
Cybersecurity LLC	2.17 (n=25)	2.73 (n=21)	2.63 (n=21)
All FY	2.44 (n=3105)	2.72 (n=3172)	2.24 (n=2938)
+New for fall 2019			
Retention Rates for Cybersecurity Communities & All First-Year Students			
Cohort*	%Fall 18 Retained to Fall 19		% Fall 17 Retained to Fall 18
Cybersecurity LC	71% (n=24)		Not available*
Cybersecurity LLC	88% (n=21)		76% (n=21)
All FY	78% (n=3176)		77% (n=2938)

**n refers to number enrolled in the earlier year*

Undergraduate Research Assessment

The assessment of the undergraduate research papers included the mentor and two of the authors reviewing the manuscripts after students completed them. All of the projects demonstrated the types of learning outcomes that the researchers anticipated. Several of the final papers were exceptional. In fact, under the direction of the faculty member leading this project, nine articles were submitted

for publication to the undergraduate research journal published by our honors college. Titles of those papers included:

- Understanding of the Use of Malware and Encryption
- Topical Review of Vulnerability Management for Local Hampton Roads Industry.
- Systemic Analysis of the Use of Artificial Intelligence (AI) in Regulating Terrorist Content on Social Media Ecosystem Using Functional Dependency Network Analysis (FDNA)
- Detection of Rouge Drones based on Radio Frequency Classification
- The Influence of Blockchain Technology on Fraud and Fake Protection
- Study of the Feasibility of a Virtual Environment for Home User Cybersecurity
- Data Breaches and Their Impact on Society
- Cognitive Resource Management in 5G Networks.
- Application of Quantaum Cryptography to Cybersecurity and Critical Infrastructures in Space Communications.

A review of the studies produced by students suggests that the undergraduate research projects were quite successful. There were, however, challenges encountered. For example, keeping students on a timeline that worked for them and the project was difficult. Also, motivating all students was problematic. In fact, four undergraduates who were initially supported on undergraduate research projects never finished their projects because they left the school. In addition, identifying appropriate mentors proved to be time consuming.

Three patterns stood out in our efforts and possibly differentiate our undergraduate research programming from many other disciplines. First, the interdisciplinary nature of cybersecurity resulted in projects from a wide range of perspectives, with research topics ranging from cybersex crimes and cyberbullying to blockchain security and securing wireless computing. Second, because the breadth of topics required us to call upon mentors from outside our cybersecurity research group, and our institution for that matter, students were exposed to a wider range of mentors. Third, the location of the research was quite varied, with some of carried out in research labs, and other projects conducted in the library or in students' homes. For many hard science research projects, such a luxury does not exist.

Internship Assessment

The internships were not easy to administer. The biggest challenge was helping students locate internship partners. Three steps were followed to develop the partnerships. First, the cybersecurity faculty reached out to businesses the faculty

have been working with since 2015. Those contacts provided a valuable source of possible interns. Second, the program coordinator worked with Career Development Services to expand the number of possible business partners. The newness of the program, however, meant that the central career office had very few contacts to share. Third, the institution reached out to a regional non-profit specializing in internship placements and coordinated strategies to introduce students to the non-profit. Collectively, these efforts took time and did not ensure that all students would easily find internship placements. As others have noted, programs must build relationships with external partners willing to hire cybersecurity interns (Tsado, 2019). With a three-year track record of placing cybersecurity interns, the cybersecurity program is building some longstanding partnerships that will help to minimize this challenge. More importantly, these partnerships will bring significant value to our students.

To assess the internships, the authors reviewed the research papers submitted by the students. This review suggested that the learning outcomes were met for each intern. Without fail, all of the students had positive things to say about the internships. Students highlighted the value of current work experience and the way the internships prepared them for their futures. The first three comments below from cybersecurity interns emphasize the work experience and last two show the focus on the future.

- "So far I love this internship. This has been the best working experience I have ever had when comparing it to my jobs in the past. I hope in the future I get a call to come back as a full-time employee. Before my internship is over I plan to sit with each of my supervisors to ask them what things I did good and bad on and what I can improve on and what I should continue to do."
- "In reflection, this internship has pushed me out of my comfort zone and made me challenge all my goals I set forth for myself upon entering college. I am grateful for all the skills and real-world work experience it has given me the opportunity to participate in. I have learned skills that I can easily apply to future interviews and jobs. I have now been able to apply what I learned from the internship to my higher-level course. This internship has truly tested my abilities and made me more confident in myself to strive to be the best I can be."
- "I was able to get my foot in the door with a company that I never knew about until this past year. The company showed me how to extract different devices, such as phones, tablets, drones, and computers. They gave me experience with Cellebrite, Blacklight, and Susteen which are huge companies in the field. I got a background on the computer forensics fundamentals and a certification that can lead me to the big

certification that companies pay a lot of money for in the forensics world Cellebrite Certified Physical Analyst."

- "My internship will influence the rest of my college career. I plan on staying at this internship until I graduate from college with my bachelors. Anytime that I learn something in class I can take that knowledge and reinforce it at my internship. This helps me expand my knowledge greatly."
- "The internship prepared me for the real world. I was able to increase my technological vocabulary. I was able to learn new things daily through tickets assigned to me and accompany staff members. It also made me realize that I picked the right career."

Service Learning Assessment

After completing the service learning projects, students (n=52) completed an online survey assessing their experiences with the assignments. Items on the survey, recommended by the Office of Service Learning and Civic Engagement, came from a survey constructed by the University of Georgia's Office of Service Learning (n.d.). Table 4 summarizes those findings. The results suggest an overwhelmingly favorable response on the part of students. For example, 98 percent agreed or strongly agreed that "It will be important for me to apply academic knowledge to community problems in the future." In addition, eight out of ten students agreed or strongly agreed that "I learned more in this course than in other courses I have taken in this discipline that DID NOT include a service-learning component." The same proportion of students agreed or strongly agreed that "The service-learning component of this course: - Positively influences my intention to complete my degree." In addition, 87 percent agreed or strongly agreed that "The service-learning component of this course: - Encouraged me to consider perspectives other than my own." The same percentage of students agreed or strongly agreed that "The service-learning component of this course: - Enhanced my ability to work as a member of a team." Collectively, these responses suggest that the cybersecurity students who participated in service learning projects benefitted from them.

In addition, students provided rich qualitative feedback showing the value of the service learning assignments. Here are a few comments students made:

- Good way to apply knowledge to a real-world application. Reinforces what I've learned as I attempt to convey the same information to others in way that is easily understood.
- I believe that it was a great experience, different than any other class that I have taken.
- I liked it, even though it was stressful…giving back to the community is always a joy!

- Offer more classes with service learning. It is a great way to get hands on experience for a class.

Table 4. Cybersecurity Students' Perceptions about Service Learning

Statements	Strongly Agree	Agree	Disagree	Strongly Disagree
It will be important for me to apply academic knowledge to community problems in the future.	20 (43.5)	25 (54.3)	1 (2.2)	
I learned more in this course than in other courses I have taken in this discipline that DID NOT include a service-learning component.	16 (38.1)	18 (42.9)	8 (19.0)	
The service-learning component of this course: - Positively influences my intention to complete my degree.	18 (34.6)	24 (46.2)	8 (15.4)	2 (2.6)
The service-learning component of this course: - Encouraged me to consider perspectives other than my own."	16 (30.8)	29 (55.8)	4 (7.7)	3 (5.8)
The service-learning component of this course: - Enhanced my ability to work as a member of a team."		26 (50.0)	4 (7.7)	3 (5.8)

Survey items from University of Georgia Office of Service Learning

While the cybersecurity service learning programming was successful, we encountered a number of challenges implementing the efforts. The biggest challenge was identifying community partners. On two different occasions, the amount of effort required by community partners to participate in "reciprocal learning" was too large and the partners declined the invitation to participate several weeks after initially agreeing. In those cases, we had to locate other assignments for the students. Another challenge that arose was that faculty were not fully aware of the principles of service learning. This was easy to overcome with faculty support provided from various units. Still, returning to Sigmon's (1994) typology, our efforts might be better seen as service LEARNING rather than "SERVICE LEARNING," given that more of our focus was given to learning than service. Despite these challenges, the overall success of the service learning activities is commendable.

Electronic Portfolio Assessment

As part of a broader study on ePortfolios (ePs), cybersecurity students were asked to provide feedback about their perceptions of ePortfolios (Payne et al., 2020). Though a handful of students were not supportive of the portfolios, the vast majority were supportive. Those particularly opposed to the strategy were older students. Table 5 shows the specific way cybersecurity students responded to the ePortfolio items included on the survey. A few findings are worth highlighting. First, two-thirds of the cybersecurity majors responding to the survey indicated they had developed an ePortfolio (31 out of 47 students providing feedback). Second, nearly two-thirds of cybersecurity majors who completed an ePortfolio indicated they believed it would help them get a job. Third, two-thirds of the majors completing ePortfolios said that it was easier to create than expected. Fourth, about the same percentage said it would have been helpful to have more courses using electronic portfolios in their first two years. Finally, eighty-three percent said they planned to update their ePortfolio in the future.

Table 5. Cybersecurity Student Perceptions about Electronic Portfolios

Statements	Strongly Agree	Agree	Disagree	Strongly Disagree
Developing an eP helped me learn about topics in my major.	5 (16.7)	7 (23.3)	12 (40.0)	6 (20.0)
My eP will help me find a job in the future.	6 (20.0)	13 (43.3)	9 (26.7)	3 (10.0)
Developing an eP helped me see connections between my courses.	5 (16.7)	11 (36.7)	10 (33.3)	4 (13.3)
Creating an eP was easier than I expected.	7 (25.3)	13 (43.3)	6 (20.0)	4 (13.3)
I plan to update my eP in the future.	10 (33.3)	15 (50.0_	3 (10.0)	2 (6.7)
I looked at sample ePs to help me figure out how to create my own.	8 (26.7)	15 (50.0)	5 (16.7)	2 (6.7)
I'm not comfortable sharing my eP with others.	1 (3.3)	8 (26.7)	15 (50.0)	8 (20.0)
It would have been helpful to use ePs more in my first or second year of college.	10 (35.7)	10 (35.7)	6 (21.4)	2 (7.1)

Students were also asked who they shared their electronic portfolios with. The vast majority (n=28) indicated sharing it with their course faculty member, and fewer said they shared it with another faculty member (n=4), family members (n=4), and possible employers (n=4). A third of the cybersecurity students (n=10) completing electronic portfolios made them public. Analyses showed a relationship between perceptions that the ePortfolio would help find a job and the ePortfolio helped the students see connections between the classes (Pearson=.875, p<.001). In addition, a negative relationship was found between the belief that ePortfolio would help find a job and the belied that the ePortfolio was a waste of time (Pearson = -.794, p <.001), suggesting that those who saw it as helpful in preparing for a career, not surprisingly, did not see the process as a waste of time. Somewhat related, questions about digital identities supported the need to develop ePortfolios. Being confident about getting a job was correlated with being satisfied with one's digital identity (Pearson = .31, $p < .05$), feeling that their digital identity shows they had a positive attitude (Pearson = .580, $p < .001$), and that their digital identity showed they have positive qualities (Pearson = .538, $p < .001$).

Another finding that stands out is that cybersecurity students were far more likely than some other majors in the study to report developing an ePortfolio. There is a simple reason for this finding – the ePortfolio is required in cybersecurity courses, but not in criminal justice or other programs. Incidentally, the only major with comparable ePortfolio usage was leadership, which also requires a capstone ePortfolio project. What this may suggest is that students and faculty will not voluntarily embrace or produce ePortfolios, even when informed of its benefits. Instead, programmatic decisions requiring their use are helpful in promoting the development and use of ePortfolios.

It is important to note that not all students reported positive reactions to ePortfolios. A sizeable percentage (just over a third) said developing the ePortfolio was a complete waste of time and just under half said that the portfolios did not help them see the connections between the courses. These findings are more likely attributed to the way the process unfolded than to the nature of ePortfolios. With faculty being new to ePortfolios, they may not have explained or carried out the purpose of the tools as effectively as they might now be able to do. Despite these findings, the overall reaction that students and faculty had to the ePortfolios was positive.

Case Study – What Worked and Didn't Work?

The authors' experiences show that high impact practices can be integrated into the cybersecurity curriculum. The practices are not panaceas but the evidence suggests they are worthwhile. Tying together the findings from our assessment with broader research on high impact practices, a number of recommendations are made to help

faculty more seamlessly integrate high impact practices into their curriculum. Table 6 summarizes "what worked" and "what didn't work" in our efforts to apply high impact practices to cybersecurity.

Table 6. What Worked and Didn't Work in the High Impact Practices

	What Worked	What Didn't Work
Freshman Learning Communities	Field trips Connected to gen ed courses	Space and time considerations in assigning classrooms
Sophomore Learning Communities	Crosslisting courses with non-SLC section	Requiring certain students to enroll Including upper level course
Living Learning Communities	Orientation course attached Developing a lab and classroom for students	Space and time considerations in assigning classrooms
Internships	Integrating written assignments with the internship Partnerships with businesses Requiring internships	Placement was sometimes difficult Certifications needed for some jobs Timing of work needs is not on a semester calendar
Undergraduate Research	Solid research produced, with some published in undergraduate research journal Demonstrated interest in additional projects	Not all students completed their projects Locating Mentors
Service Learning	Contributed to meaningful projects Student presentations Connected to a writing project	Finding service learning mentors Creating meaning for students
ePortfolios	Enhanced digital confidence Deeper learning Support for students	Connecting the ePortfolio across classes Demonstrating the purpose of ePortfolios

Regarding the learning communities, the authors noted that different types of learning communities (FLC, SLC, LLC) required different decisions. Freshmen

learning communities worked well when connected with general education courses that had field trips embedded. Sophomore learning communities worked best when crosslisting the SLC section with a non-SLC section. The living learning community benefitted from an orientation course and a lab installed in the residence hall. Across the learning communities, issues that arose included obstacles working with central registration to assign classrooms and unsuccessful efforts requiring certain students to enroll in the learning communities.

Internship programming appeared to benefit from the written assignments included in the requirements. These assignments forced students to connect their course material with their course experiences. In addition, requiring the internships (rather than making them electives) ensured that students would gain work-related skills in their coursework. A history of business partnerships helped to administer the programs, though, as noted above, it was sometimes hard for students to find internships. Students without required certifications, for example, reported problems finding internships. Also, combining the semester calendar with a business calendar was sometimes problematic.

The undergraduate research projects involved a wide range of empirical approaches. Students appeared to work hard when told they could submit their projects to a journal. Some even expressed interest in additional research interests. Problems arose in some cases keeping students motivated and interested in research. In addition, locating research mentors was sometimes problematic.

Service learning assignments worked well when meaningful assignments were identified for students to work on. Also, having students do presentations on their service learning projects seemed to make them take ownership over their learning. Connecting the service learning to a writing assignment ensured that knowledge from the course was integrated into the service learning. Issues confronted included finding service learning mentors and, if the project was not automatically meaningful for students, getting students interested in the assignments.

Electronic portfolios worked well in that they enhanced students' digital confidence and promoted deeper learning. The portfolio process worked better as a result of student support that was provided by the Center for High Impact Practice. Problems arose when students saw the portfolios as a waste of time. Also, getting faculty across classes to use electronic portfolios was challenging.

IMPLICATIONS

Based on our experiences, seven recommendations are offered to help other cybersecurity programs develop and implement high impact practices in cybersecurity courses. These include integrating experiential learning throughout the curriculum, developing campus-wide partnerships, embracing the

interdisciplinary nature of cybersecurity, demonstrating the purpose of the high impact practices, providing faculty development, emphasizing student writing, and embracing failure.

Integrating experiential learning throughout the curriculum. One common feature of the high impact practices utilized in our efforts is their foundation in experiential learning. Calls for experiential learning in cybersecurity courses bolster our recommendation that high impact practices become a staple in cybersecurity courses. Indeed, experiential learning has been hailed as "the cornerstone in educating the future workforce in cybersecurity" (Justice & Vyas, 2017, np). Research shows that experiential learning activities for cybersecurity students improves student learning and self-efficacy (Konak, 2018). Active learning and hands-on activities are at the core of many national initiatives promoting cybersecurity education. GenCyber summer camps, for example, strongly integrate experiential learning activities into summer programs funded by the National Security Agency (Payne et al., 2016). Experiential learning strategies can be integrated into a wide range of cybersecurity teaching practices including case studies (Cai & Arney, 2018), collaborative assignments (Konak & Bartolacci, 2016), laboratory assignments (Ledford et al., 2016), and simulations (Burris et al., 2018). As well, experiential learning can, and should, be integrated in cybersecurity curricula – from the very first course cybersecurity majors take to the very last one. As emphasized above, ePortfolios provide one opportunity to connect the experiences of the students from different courses, along with the demonstration of their learning.

Developing campus-wide partnerships. Throughout this discussion, it should be clear that we were not able to carry out the implementation of these high impact practices in a vacuum. In addition to faculty who came from seven different academic departments, the following units helped in varying levels in developing and implementing the high impact practices: Career Development Services, Center for High Impact Practices, ePortfolios and Digital Initiatives Program, Impact Learning Communities Program, the Graduate School, Housing and Residence Life, Information and Technology Services, Office of Institutional Effectiveness and Assessment, Office of Undergraduate Research, the Registrar's Office, and the Service Learning and Civic Engagement Program. The importance of cross-campus partnerships in developing and implementing high impact practices in cybersecurity programming cannot be understated.

Embracing the interdisciplinary nature of cybersecurity. Scholars have long recognized that cybersecurity is an interdisciplinary field drawing from a wide range of disciplines (Tsado, 2019). While some high impact practices might be developed within specific disciplinary silos, others are stronger when interdisciplinarity is embraced. Learning communities, for example, linking

together an introductory cybersecurity course and a general education course such as English or Communications, could help students understand the importance of those fields in the cybersecurity major. Electronic portfolios developed over the student's academic career will be much richer if they pull in various disciplines and synthesize their learning experiences. Cybersecurity service learning assignments integrating students from multiple majors have strong appeal. In the end, students benefit significantly from the integration of interdisciplinary efforts and high impact practices. We may need to look to general education courses. One anecdotal comment from a student in her internship paper showed that the student learned about the value of interdisciplinary cybersecurity courses through the internship. She made the following comments:

> Interdisciplinary studies was an interesting course taken. In the beginning, I did not realize how important it would be in the workplace. In the workplace there are people with different backgrounds and some people may find it difficult to relate or communicate with each other. Gender, race, religion, and ethnic backgrounds all contribute to the work environment. Taking this course benefited me in the workplace when working with other people who were different.

Demonstrating the purpose of the high impact practices. It is also important that cybersecurity faculty identify and communicate the purpose of the various high impact practices for students. Absent any direction from faculty, students will create their own reasons for the high impact practices, and their perceptions may not align with the overall purpose of the high impact practices. If ePortfolios, for example, are designed in a course for the purpose of promoting deeper learning, but the student believes the purpose is to simply showcase the material, the ultimate benefit of the high impact practice is minimized. As another example, if a student thinks the purpose of an internship is to learn work skills, rather than to learn through the application of course materials to the work environment, the internship experience may not be fully realized. In identifying the purpose of the high impact practices, faculty should recognize that the purpose is derived from the student learning outcomes of a specific course or program.

Providing faculty development. It likely seems obvious to state this, but we make the recommendation nonetheless – faculty must be trained how to effectively use high impact practices. It is no secret that faculty receive virtually no training on how to teach in their graduate school careers and others have called for faculty development in related cybersecurity topics (Belshaw, 2019). Expecting them to become experts with evidence-based practices without giving them the support they need makes as much sense as expecting our students to become cybersecurity experts without ever teaching them about the fundamentals of cybersecurity. Many

institutions have faculty development centers or other units able to provide some support. Where those do not exist, program leaders are encouraged to explore new ways to provide faculty development to their faculty.

Emphasizing student writing. Another recommendation has to do with student writing. One consistent practice across the implementation of our high impact practices was the inclusion of writing assignments. Doing service learning, completing internships, creating ePortfolios, engaging in learning communities, and researching cybersecurity topics are meaningful experiences. It is not until students reflect on those experiences through writing about them that they truly engage in the deep learning that makes a difference in their lives. Their ability to write about their high impact practices experiences will serve them well.

Embracing failure. The final recommendation has to do with failure. More specifically, in expanding high impact practices into curricula where such practices have not been used, faculty should embrace failure (of their own efforts, not of the students!). The failures encountered by the authors are illustrative and are offered here to help others avoid them. For example, learning community classes were not as connected to one another as they ideally should have been at the beginning of the process. A handful of the undergraduate researchers who were chosen (e.g., those who dropped out) probably should not have been selected in the first place. The leadership team significantly underestimated how much work it would take to get faculty and students to buy in to the value of electronic portfolios. In a similar way, developing service learning assignments was an arduous task, which resulted in some of the assignments potentially being of limited value to some students and the community.

The cybersecurity team learned form these setbacks and used them to shape subsequent programming. The implementation of the high impact practices in the cybersecurity curriculum continues to evolve. While far from perfect, these efforts provide meaningful and impactful results not typically found in traditional teaching strategies.

ACKNOWLEDGEMENTS

This research is supported in part by the National Science Foundation under grant DGE-1723635.

REFERENCES

Alexiou, A., & Paraskeva, F. (2010). Enhancing self-regulated learning skills through the implementation of an e-portfolio tool. *Procedia-Social and Behavioral Sciences*, *2*(2), 3048-3054.

Andrade, M. S. (2007). Learning communities: Examining positive outcomes. *Journal of College Student Retention: Research, Theory & Practice*, *9*(1), 1-20.

Belshaw, S. H. (2019). Next generation of evidence collecting: The need for digital forensics in criminal justice education. *Journal of Cybersecurity Education, Research and Practice*, *2019*(1), 3.

Bhattacharya, M., & Hartnett, M. (2007, October). E-portfolio assessment in higher education. In *2007 37th annual frontiers in education conference-global engineering: knowledge without borders, opportunities without passports* (pp. T1G-19). IEEE.

Bokser, J. A., Brown, S., Chaden, C., Moore, M., Cleary, M. N., Reed, S., & Wozniak, K. (2016). Finding Common Ground: Identifying and Eliciting Metacognition in ePortfolios across Contexts. *International Journal of ePortfolio*, *6*(1), 33-44.

Bonet, G., & Walters, B. R. (2016). High impact practices: Student engagement and retention. *College Student Journal*, *50*(2), 224-235.

Burris, J., Deneke, W., & Maulding, B. (2018, July). Activity simulation for experiential learning in cybersecurity workforce development. In *International Conference on HCI in Business, Government, and Organizations* (pp. 17-25). Springer, Cham.

Brownell, J. E., & Swaner, L. E. (2009). High-impact practices: Applying the learning outcomes literature to the development of successful campus programs. *Peer Review*, *11*(2), 26.

Buyarski, C. A., Aaron, R. W., Hansen, M. J., Hollingsworth, C. D., Johnson, C. A., Kahn, S., & Powell, A. A. (2015). Purpose and pedagogy: A conceptual model for an ePortfolio. *Theory Into Practice*, *54*(4), 283-291.

Buzzetto-More, N. (2010). Assessing the efficacy and effectiveness of an e-portfolio used for summative assessment. *Interdisciplinary Journal of e-Learning and learning Objects*, *6* (1), 61-85.

Cai, Y., & Arney, T. (2018). Using case studies to teach cybersecurity courses. *Journal of Cybersecurity Education, Research and Practice*, *2018*(2), 3.

Cambridge, D. (2010). *Eportfolios for lifelong learning and assessment*. John Wiley & Sons.

Carlin, A., & Manson, D. (2016). Polytechnic education for the cybersecurity workforce: leaders in polytechnic education prepare the next generation with hands-on cyber risk training. *Strategic Finance*, *98*(1), 62-64.

Conefrey, T. (2018). Supporting first-generation students' adjustment to college with high-impact practices. *Journal of College Student Retention: Research, Theory & Practice*, 1521025118807402.

Crumpler, W., & Lewis, J. A. (2019). The cybersecurity workforce gap. *Center for Strategic and International Studies, Washington, DC.[Online]. Available: https://www. csis. org/analysis/cybersecurityworkforce-gap*.

Dagley, M., Georgiopoulos, M., Reece, A., & Young, C. (2016). Increasing retention and graduation rates through a STEM learning community. *Journal of College Student Retention: Research, Theory & Practice*, *18*(2), 167-182.

Dark, M. J. (2004, October). Civic responsibility and information security: An information security management, service learning course. In Proceedings of the 1st annual conference on Information security curriculum development (pp. 15-19).

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.

Eynon, B., & Gambino, L. M. (2017). *High-impact ePortfolio practice: A catalyst for student, faculty, and institutional learning*. Stylus Publishing, LLC.

Eyler, J., & Giles Jr, D. E. (1999). *Where's the learning in service-learning? Jossey-Bass Higher and Adult Education Series*. Jossey-Bass, Inc., 350 Sansome St., San Francisco, CA 94104.

Finley, A. (2011). Assessment of high-impact practices: Using findings to drive change in the compass project. *Peer Review*, *13*(2), 29.

Fink, J. E., & Inkelas, K. K. (2015). A history of learning communities within American higher education. *New Directions for Student Services*, *2015*(149), 5-15.

Frank, C. E., McGuffee, J. W., & Thomas, C. (2016). Early undergraduate cybersecurity research. *Journal of Computing Sciences in Colleges*, *32*(1), 46-51.

Furco, A. (1996). Service-learning: A balanced approach to experiential education. In *Expanding Boundaries: Serving and Learning* (pp. 2-6). Washington, DC: Corporation for National Service.

Fussell, E. (2002). Internships ensure sure footing. *INTECH*, *49*(9), 64-64.

Gebauer, R., Wade, M. E., Muller, T., Kramer, S., Leary, M., & Sopper, J. (2020). Unique strategies to foster integrative learning in residential learning communities. *Learning Communities Research and Practice*, *8*(1), 9.

Innocenzi, R. L., Brown, K., Liggit, P., Tout, S., Tanner, A., Coutilish, T., & Jenkins, R. J. (2018). "Think Before You Click. Post. Type." Lessons learned from our university cyber security awareness campaign. *Journal of Cybersecurity Education, Research and Practice*, 2018(1), 3.

Johnson, J. L. (2000). Learning communities and special efforts in the retention of university students: What works, what doesn't, and is the return worth the investment? *Journal of College Student Retention: Research, Theory & Practice*, *2*(3), 219-238.

Jones, K. S., Namin, A. S., & Armstrong, M. E. (2018). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Transactions on Computing Education (TOCE)*, *18*(3), 1-12.

Justice, C., & Vyas, R. (2017). Cybersecurity education: RunLabs rapidly create virtualized labs based on a simple configuration file. ASEE Annual Conference and Exposition.

Lenning, O. T., & Ebbers, L. H. (1999). *The Powerful Potential of Learning Communities: Improving Education for the Future. ASHE-ERIC Higher Education Report, Vol. 26, No. 6*. ERIC Clearinghouse on Higher Education, One Dupont Circle, NW, Suite 630, Washington, DC 20036-1183. Columbus, OH: Proceedings for American Society for Engineering Education.

Kapoor, A., & Gardner-McCune, C. (2020). Barriers to Securing Industry Internships in Computing. *ACE*.

Kilgo, C. A., Sheets, J. K. E., & Pascarella, E. T. (2015). The link between high-impact practices and student learning: Some longitudinal evidence. *Higher Education*, *69*(4), 509-525.

Kirk, S., Foreman, D., Lee, C., & Beasley, S. W. (2019). Sit Back, Relax, And Tell Me All Your Secrets. *Journal of Cybersecurity Education, Research and Practice*, *2019*(2), 4.

Konak, A., & Bartolacci, M. R. (2016). Using a virtual computing laboratory to foster collaborative learning for information security and information technology education. *Journal of Cybersecurity Education, Research and Practice*, *2016*(1), 2.

Konak, A. (2018). Experiential learning builds cybersecurity self-efficacy in K-12 students. *Journal of Cybersecurity Education, Research and Practice*, *2018*(1), 6.

Kuh, G. D. (2008). Excerpt from high-impact educational practices: What they are, who has access to them, and why they matter. *Association of American Colleges and Universities*, *14*(3), 28-29.

Kuh, G., O'Donnell, K., & Schneider, C. G. (2017). HIPs at ten. *Change: The Magazine of Higher Learning*, *49*(5), 8-16.

Ledford, H., Mountrouidou, X., & Li, X. (2016). Denial of service lab for experiential cybersecurity learning in primarily undergraduate institutions. *Journal of Computing Sciences in Colleges*, *32*(2), 158-164.

Lesko Jr, C. J. (2019). A design case: Assessing the functional needs for a multi-faceted cybersecurity learning space. *Journal of Cybersecurity Education, Research and Practice*, *2019*(1), 6.

McGettrick, A. (2013). Toward effective cybersecurity education. *IEEE Security & Privacy*, *11*(6), 66-68.

Mirkovic, J., & Benzel, T. (2012). Teaching cybersecurity with DeterLab. *IEEE Security & Privacy*, *10*(1), 73-76.

Morgan, S. (2016). Zero-percent cybersecurity unemployment, 1 million jobs unfulfilled. Computer Science Online. Available online at https://www.csoonline.com/article/3120998/zero-percent-cybersecurity-unemployment-1-million-jobs-unfilled.html

Payne, B.K., Paredes, T., & Cross, B. (2020). Student perceptions about the production of electronic portfolios: Technology, process, and showcase insights. Unpublished manuscript.

Payne, B. R., Abegaz, T., & Antonia, K. (2016). Planning and implementing a successful NSA-NSF Gencyber summer cyber academy. *Journal of Cybersecurity Education, Research and Practice*, 2016(2), 3.

Porter, L. A. (2017). High-impact practices in materials science education: Student research internships leading to pedagogical innovation in STEM laboratory learning activities. *MRS Advances*, *2*(31-32), 1667-1672.

Rivera, J. C., Howard, J., Goh, S., Worrell, J. L., & Di Gangi, P. (2017). Social media risk perceptions of human resource professionals. *Journal of Cybersecurity Education, Research and Practice*, *2017*(2), 3.

Settle, A., & Steinbach, T. (2018, September). Retention rates for the first three years of a linked-courses learning community. In *Proceedings of the 19th Annual SIG Conference on Information Technology Education* (pp. 166-171).

Sigmon, R.L. (1994). *Serving to learn, Learning to serve. Linking service with learning*. Council for Independent Colleges Report.

Sigmon, R. L. (1979). Service-learning: Three principles. Synergist. National Center for Service-Learning, ACTION, 8(1):9-1 1.

Simons, L., Marshall, C., Blank, N., & Weaver, N. (2020). Differences in Student Learning Outcomes that Utilize High Impact Practices. *The European Journal of Social & Behavioural Sciences*, *27*(1), 3049-3072.

Smith, B. L. (2001). The challenge of learning communities as a growing national movement. *Peer Review*, *4*(1), 4-8.

Springer, J. T., Hatcher, J., Rust, M., & Powell, A. A. (2019). Enhancing the quality of high-impact practices through taxonomies. *What Makes a Performance Indicator an Equity-Driven, High-Performance Indicator?*, *31*(2): 8.

Stanton, T.K., Giles, D. Jr, & Cruz, N. (1999). *Service-learning: A movement's pioneers reflect on its origins, practice, and future.* San Francisco: Jossey-Bass Inc.

Thompson, J. D., Herman, G. L., Scheponik, T., Oliva, L., Sherman, A., Golaszewski, E., ... & Patsourakos, K. (2018). Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews. *Journal of Cybersecurity Education, Research and Practice*, *2018*(1), 5.

Tinto, V. (1998, May). Learning communities: Building gateways to student success. In *The National Teaching and Learning Forum*, 7, 4: 1-11.

Tinto, V. (2019). Learning better together. *Transitioning Students in Higher Education: Philosophy, Pedagogy and Practice*, 2.

Tsado, L. (2019). Cybersecurity Education: The need for a top-driven, multidisciplinary, school-wide approach. *Journal of Cybersecurity Education, Research and Practice*, *2019*(1), 4.

University of Georgia Office of Service Learning SL Course Survey. (n.d.). Retrieved April 4, 2020, from https://servicelearning.uga.edu/faculty-resources/sl-surveys.

Walton, E., Carrington, S., Saggers, B., Edwards, C., & Kimani, W. (2019). What matters in learning communities for inclusive education: a cross-case analysis. *Professional Development in Education*, 1-15.

Weiss, R. S., Boesen, S., Sullivan, J. F., Locasto, M. E., Mache, J., & Nilsen, E. (2015, February). Teaching cybersecurity analysis skills in the cloud. In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education* (pp. 332-337).