Journal of Information Systems Education

Volume 32
Issue 2
Spring 2021

Cybersecurity, Technology, and Society: Developing an Interdisciplinary, Open, General Education Cybersecurity Course

Brian K. Payne, Wu He, Cong Wang, D. E. Wittkower, and Hongyi Wu

Recommended Citation: Payne, B. K., He, W., Wang, C., Wittkower, D. E., & Wu, H. (2021). Cybersecurity, Technology, and Society: Developing an Interdisciplinary, Open, General Education Cybersecurity Course. *Journal of Information Systems Education,* 32(2), 134-149.

Article Link: http://jise.org/Volume32/n2/JISEv32n2p134.html

Initial Submission: 28 May 2020
Accepted: 10 December 2020
Abstract Posted Online: 13 March 2021
Published: 9 July 2021

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Cybersecurity, Technology, and Society: Developing an Interdisciplinary, Open, General Education Cybersecurity Course

Brian K. Payne
Wu He
Cong Wang
D. E. Wittkower
Hongyi Wu
Old Dominion University
Norfolk, VA 23529, USA
bpayne@odu.edu, whe@odu.edu, c1wang@odu.edu, dwittkow@odu.edu, h1wu@odu.edu

ABSTRACT

This paper describes an interdisciplinary effort involving faculty from five different disciplines who came together to develop an interdisciplinary, open, general education cybersecurity course. The course, Cybersecurity, Technology, and Society, brings together ideas from interdisciplinary studies, information technology, engineering, business, computer science, criminal justice, and philosophy to provide students an interdisciplinary introduction to cybersecurity. We provide an overview of the rationale for the course, the process the authors went through developing the course, a summary of the course modules, details about the open education resources used as readings, and the types of assignments included in the class. We conclude by offering recommendations for others developing similar courses.

Keywords: Cybersecurity, General education, Instructional pedagogy, Integrative learning

1. INTRODUCTION

Concern about cybersecurity has grown dramatically over the past decade. This increased concern stems, in part, on the way technology has reshaped our existence. Estimates suggest that individuals now spend up to half a day in front of electronic media (Fisher, 2019). The U.S. Department of Commerce (2020) reports that $601.7 billion was spent on retail e-commerce in 2019. Individuals are able to meet new friends, romantic partners, and future spouses by swiping right on their handheld devices. Countless hours are spent streaming movies on Netflix or Amazon, surfing the internet, and posting on social media. Students are now able to earn their entire degrees online.

However, it's not just our behavior that has changed. Our seemingly paradoxical concerns about privacy (Hargittai and Marwick, 2016; Hallam and Zanella, 2017; Wittkower, 2020), interest in certain types of products (Chesnes and Jin, 2019), and attitudes about different political issues (Anduiza et al., 2012; Bimber et al., 2015) are related to the way reality has shifted to take place within digital media. The way we express our interest in various sporting activities (Kim et al., 2019; O'Hallarn et al., 2019), our preference for educational strategies (Krug et al., 2016; Lee, Stringer, and Du, 2017), how we teach our courses (Case et al., 2019; Goh, Di Gangi, and Gunnells, 2020), and the way we sleep (LeBourgeois et al., 2017; Scott and Woods, 2019) are shaped by the same information and communication technologies. Scholars across multiple disciplines are exploring the connections between technological change and human nature (Jonas, 1979; Hefner, 2003; Vicente, 2010) and have identified a wide range of risks and vulnerabilities from these changes.

These risks and vulnerabilities have led to an increased call for more cybersecurity professionals (Nodeland, Belshaw, and Saber, 2019; Wang and D'Cruze, 2019). At the close of 2020, there were more than half a million unfilled cybersecurity jobs in the United States (Cyberseek.org, 2020). Qualified cybersecurity professionals aren't just magically produced. Rather, educational institutions have been called upon to develop educational programming to meet this enormous level of demand. New and revised degree programs, courses, and certificates have grown, though perhaps not as quickly as the number of new jobs.

In addition to the call for a more robust cybersecurity workforce, cybersecurity experts have highlighted three themes: (1) cybersecurity should be addressed as an interdisciplinary topic (Hoffman, Burley, and Toregas, 2011; Weiss et al., 2020), (2) educational and awareness campaigns should target as many individuals as possible (Dupuis, 2017; Kostyuk and Wayne, 2020), and (3) cybersecurity solutions must balance human factors and technical issues (Rege, Williams, and Mendlein, 2019). Guided by these themes and responding to the impact of ongoing technological change, the Center for Cybersecurity Education and Research at Old Dominion University created an introductory, interdisciplinary, general education course titled Cybersecurity, Technology, and Society.

Several practical reasons warranted the development of this course. First, it was recognized that general education courses are a good way to attract new majors (Alvin, 2019). Second, as others have noted, general education courses in cybersecurity have the potential to support efforts focused on "recruiting a greater diversity of students" (Mountrouidou, Li, and Burke, 2018, p. 182). Third, general education courses respond to suggestions that widespread education about cybersecurity is needed because of the relevance that cybersecurity has for so many different careers and professions (Jacob, Peters, and Yang, 2019), including those specific to the cybersecurity workforce (Fulton, Lawrence, and Clouse, 2013; Knapp, Maurer, and Plachkinova, 2017). Fourth, from our perspective, having a general education course in cybersecurity helps to show what we value as a university. Fifth, a cybersecurity general education course helps to educate students how to protect the university's computer and networking environment. Such awareness is critical to protecting the "business side" of a university's cyber infrastructure (see Vasileiou and Furnell, 2019). Sixth, it was believed that the course would help to attract women and minorities to the cybersecurity major from the broadening participation perspective. After all, interdisciplinary efforts, in particular, are believed to promote inclusive thinking (Moll, 2020) and be more attractive to women and minorities (Rhoten and Pfirman, 2007; Atkinson and Mayo, 2010; Goonewardene et al., 2016). Finally, the value of introductory cybersecurity courses as a mechanism to "educate the masses" about cybersecurity has been highlighted in the cybersecurity literature (Dupuis, 2017), with some research showing that undergraduate students are part of the "weakest link" when it comes to cybersecurity (Yan et al., 2018).

In this paper, we describe the interdisciplinary cybersecurity course we developed. Specific attention is given to the course background, the course modules, the open educational resources used as reading materials, and recommendations for others developing similar courses.

In 2015, Old Dominion University created the Center for Cybersecurity Education and Research as an interdisciplinary unit designed to bring together faculty to offer cybersecurity courses and conduct cutting-edge research. The same year, the faculty affiliated with the Center created an interdisciplinary cybersecurity major, with 11 students enrolling in the major. The major subsequently evolved into a standalone, interdisciplinary Bachelor's degree program with focus areas in cybersecurity, an NSA-CAE recognized program in cyber operations, as well as an interdisciplinary program in cybercrime. Currently, more than 600 students are enrolled in these programs. Across the programs, courses come from a range of disciplines, including computer engineering, computer science, philosophy, political science, criminal justice, business, interdisciplinary studies, cybersecurity, and information technology.

Recognizing the need to give cybersecurity majors a consistent introduction to cybersecurity through an interdisciplinary lens while simultaneously recruiting new majors to the program, in 2017-2018, five faculty from the Center came together to create *Cybersecurity, Technology, and Society*. These faculty included a computer engineer (Wu), philosopher (Wittkower), computer scientist (Wang), business information technology professor (He), and a criminologist (Payne). The faculty agreed on five aspects of the course: (1) it must be grounded in interdisciplinary themes, (2) it must be developed in a way that students from various backgrounds would be able to successfully complete the class, (3) it must use open educational resources as reading materials, (4) it must be made available in an open format for others to use, and (5) each disciplinary area should be equally emphasized through an interdisciplinary lens. In the planning stages, we reviewed the university's general education requirements and identified the "Ways of Knowing Impact of Technology" area as the most appropriate area for our interdisciplinary course. This part of our general education requirements is based on the following description provided in our catalogue:

> It is important for students to understand not only how a technology functions, but also how technology affects society. These courses are intended to develop students' abilities to make reasoned judgments about the impact of technological development upon world cultures and the environment as well as upon individuals and societies.

The faculty worked together to create a syllabus and a plan for developing the course. In getting it approved by the university, we completed the necessary paperwork identifying our course description, showing how our course would meet the learning outcomes the university has set for the Impact of Technology area, and providing a sample syllabus. The course description for the course was kept simple to make it easier for faculty from across disciplines to teach the class. The course description we developed is: "Students will explore how technology is related to cybersecurity from an interdisciplinary orientation. Attention is given to the way that technologically-driven cybersecurity issues are connected to cultural, political, legal, ethical, and business domains."

Table 1 shows the learning outcomes prescribed by the university and the learning outcomes we developed for Cybersecurity, Technology, and Society. As shown in the table, our learning outcomes align directly with the university's outcomes for the Impact of Technology requirement. In fact, the university's guidance helped to formulate the entire class in a way that serves the needs of our majors, non-majors, the undergraduate program, and the community at large. Subsequently, we also engaged an instructional designer to provide guidance on the actual course design and development.

University Gen Ed Technology Learning Outcomes	**Cybersecurity, Technology, and Society Outcomes**
Upon completing this gen ed area, students will be able to: • Describe the use and development of a given technology as a human and cultured activity. • Understand and describe the components, mechanisms, and function of a technological system, such as information and communication, finance, energy production, industrial production, food production, international trade, transportation, education, etc. • Discuss the impact that a given technology may have on its users: how it may change users' conception of reality and what users' perceptions and biases are toward it. • Understand and describe the potential consequences, both intended and unintended, of a given technology for individuals, nations, societies, and the environment. • Express informed opinions about the cost/benefit relationship of a given technology, with considerations for development or controlled limitations. • Understand and describe how technology has enabled the pace of change and interdependency that have accelerated globalization. • Describe the role of technology in defining ideas of progress and modernism.	Upon completing this class, students will be able to: • Describe how cyber technology creates opportunities for criminal behavior. • Identify how cultural beliefs interact with technology to impact cybersecurity strategies. • Understand and describe how the components, mechanisms, and functions of cyber systems produce security concerns. • Discuss the impact that cyber technology has on individuals' experiences with crime and victimization. • Understand and describe ethical dilemmas, both intended and unintended, that cybersecurity efforts produce for individuals, nations, societies, and the environment. • Describe the costs and benefits of producing secure cyber technologies. • Understand and describe the global nature of cybersecurity and the way that cybersecurity efforts have produced and inhibited global changes. • Describe the role of cybersecurity in defining definitions of appropriate and inappropriate behavior. • Describe how cybersecurity produces ideas of progress and modernism.

Table 1. General Education Technology Learning Outcomes and Course Learning Outcomes

2. COURSE MODULES

Table 2 provides a list of the seven modules and their accompanying learning outcomes. These learning outcomes represent the five participating faculty members' expertise areas, with the caveat that we are also growing experts in the area of interdisciplinary studies. The faculty members worked on the modules independently initially, with changes later made to integrate the modules together. Table 2 also shows the broader learning outcomes of the program. While this course aligns with those broader program outcomes, it is not expected to meet each of those program outcomes as the other courses in the program would be contributing to the same program outcomes.

Module 1: Introduction to Cybersecurity Through an Interdisciplinary Lens • Define cybersecurity, • Describe how cybersecurity affects our daily lives. • Identify disciplines that affect and are affected by cybersecurity principles and design. • Set up an ePortfolio. • Describe why cybersecurity is an interdisciplinary societal issue. • Describe associated disciplines related to cybersecurity. • Identify various pathways to careers in cybersecurity.	**Module 5. Computer Science and Cybersecurity** • Describe how the discipline of computer science is related to cybersecurity. • Compare and contrast authentication and authorization. • Identify the three objectives of information security. • Describe three firewall protection services. • Provide examples about when to use encryption.
Module 2: Information Technology and Cybersecurity • Describe how the discipline of information technology relates to cybersecurity. • Define information security • Compare and contrast exposure, threat, and vulnerability. • Identify three types of security controls • Explain the importance of cybersecurity policy and training • Identify how cultural beliefs interact with technology to impact cybersecurity strategies.	**Module 6. Criminal Justice and Cybersecurity** • Discuss the impact that cyber technology has on individuals' experiences with crime and victimization. • Describe the role of cybersecurity in defining definitions of appropriate and inappropriate behavior. • Describe the role of the justice system in cybercrime cases. • Identify common cybercrimes and theories explaining them. • Explain how the discipline of criminal justice addresses cybercrime.
Module 3. Engineering and Cybersecurity • Discuss the impact of cyber technology on engineering systems. • Identify common vulnerabilities in engineering cyber systems. • Discuss impact of attacks on engineering systems.	**Module 7. Philosophy and Cybersecurity** • Describe how the discipline of philosophy is related to cybersecurity. • Describe the role of cybersecurity in defining definitions of appropriate and inappropriate behavior.

• Describe fundamental design principles for securing engineering cyber systems. • Understand and describe how the components, mechanisms, and functions of cyber systems produce security concerns.	• Describe how cybersecurity produces ideas of progress and modernism. • Understand and describe ethical dilemmas, both intended and unintended, that cybersecurity efforts produce for individuals, nations, societies, and the environment.
Module 4. Business and Cybersecurity • Describe how cybersecurity relates to business. • Define the concept "white-collar cybercrime." • Describe why cybersecurity should matter to businesses. • Identify three types of cybersecurity businesses. • Compare/contrast white-collar crime/cybercrime. • Describe the roles of customers, workers, and leaders in cybersecurity. • Describe the costs and benefits of producing secure cyber technologies.	**Program Outcomes** • Integrate insights from other disciplines to address a cybersecurity topic. • Appropriately communicate complex topics in diverse organizational settings. • Promptly apply interdisciplinary research process. • Explain impact of technology from historical perspective and its potential future impact. • Understand the security landscape by identifying threats, vulnerabilities, and controls.

Table 2. Learning Outcomes for Each Module and the BS Program

2.1 Module 1: Introduction to Cybersecurity through an Interdisciplinary Lens

The first module provides an introduction to cybersecurity. The module begins by addressing what is meant by the term "cybersecurity" through an interdisciplinary framework. Attention is given to the fact that cybersecurity can be defined as any of the following:

- An interdisciplinary field of study
- An academic major
- A process
- A social problem
- A business problem
- A privacy issue
- An individual concern
- A possible business
- A possible career

Different than traditional introductions to the topic, this module addresses cybersecurity through an interdisciplinary lens. It is inarguable that cybersecurity is best approached through a multidisciplinary lens (Tsado, 2019). Indeed, a 2010 National Science Foundation workshop including cybersecurity experts highlighted the need to address the topic through an interdisciplinary lens (Hoffman, Burley, and Toregas, 2011).

Scholars have noted that traditional cybersecurity coursework often overlooks the "human element" (Rege, Williams, and Mendlein, 2019). In the words of one author team,

> What we have not dealt with is the human behavior and creative thinking that characterizes the exploits of the hacker community, and until the solution incorporates actions that recognize and address every reasonable form of attack, we will never be secure (Shoemaker and Kohnke, 2016, p. 12).

Such an oversight is problematic because the vast majority of cybersecurity incidents, if not all of them, can be traced to decisions or behaviors by humans (Lebek et al., 2014). A technical approach to cybersecurity focuses on how to use technology to secure cyberspace. A humanistic approach focuses on the types of issues humans face with the widespread integration of technology into our daily lives. Describing the value of bringing the social sciences into cybersecurity education, one professor concluded,

> Cybersecurity professionals can continue to chase the incidents that come their way, but it will become more beneficial to begin looking for the root of the problems faced. An interdisciplinary approach leverages insight from all areas to provide a more integrated and realistic foundation for understanding cybersecurity (Stockman, 2013, p. 121).

The cybersecurity literature embracing interdisciplinarity was useful in developing the first module. In addition, the broader literature on interdisciplinary studies was useful in conveying the value of these approaches. Repko, Szostak, and Buchberger's (2014) definitions of multidisciplinarity, ("Placing side by side the insights from two or more disciplines without attempting to integrate them" (p. 2)), transdisciplinarity ("Involves academic researchers from different, unrelated disciplines as well as non-academic participants (i.e., stakeholders or user) to create new knowledge" (p. 35)), and interdisciplinarity ("A cognitive process by which individuals or groups draw on disciplinary perspectives and integrate their insights to advance their understanding of a complex problem with the goal of applying the understanding to a real-world problem" (p. 32)) are included to distinguish among the different approaches for the students. The benefits of such an interdisciplinary approach for students, universities, and the community are considered. After reviewing multiple definitions, the module concludes with an overview of the way that the following fields help to make up the interdisciplinary study of cybersecurity: information technology, engineering, computer science, criminal justice/criminology, sociology, philosophy, psychology, victimology, leadership, and law.

2.2 Module 2: Information Technology and Cybersecurity

The second module introduces students to cybersecurity through an information technology framework. The material connects cybersecurity to the discipline of information technology within the interdisciplinary framework. As information systems scholars point out, cybersecurity is "both a business and technical issue" (Logan, 2020, p. 178). With this overlap in mind, the module was designed to encourage students to see the connections between "information security" and "cybersecurity." In addition, specific attention is given to defining information cybersecurity – as a form of cybersecurity, the concepts of threat, vulnerability, and exposure are reviewed. Types of security controls are considered along with the importance of a general understanding about cybersecurity policy and training. Tied into the discussion is the underlying implication that cultural and subcultural beliefs interact with technology to produce cybersecurity strategies and policies.

The fundamental basis of this module is grounded in the recognition that information technology, as a field, has a multifaceted relationship with cybersecurity. Information technology is identified as involving both computer technology and communications technology. A distinction is made between information security (protecting data) and information security management (the business process for protecting data) (Whitman and Mattord, 2011). Also stressed in this module is the point that information technology is related to the disciplines discussed in subsequent modules. Such a conclusion is supported by scholars who point to the interdependency between information systems and other disciplines, and computing disciplines in particular (Topi, 2019).

The module includes a discussion of the National Institute of Standards and Technology (NIST) framework to help students understand how NIST recommends managing cybersecurity related risks in businesses and agencies. The information security triad (confidentiality, integrity, and availability) is reviewed to help students understand the way that companies, businesses, and agencies are expected to protect information/data. The important distinction between identification (asserting identity) and authentication (confirming identity) is considered. Different authentication strategies are considered as well as the physical security strategies (e.g., locked doors, cameras, securing equipment, employee training) needed to protect data. Students also learn about the core activities of the NIST framework.

2.3 Module 3: Engineering and Cybersecurity

The third module explores cybersecurity through an engineering framework. The basic premise on which the module is based is that systems and technologies must be engineered securely in order to foster "the security and well-being of societies and economies" (Konstantinou and Mohanty, 2020, p. 10). Such a premise connects the engineering module to the other modules: the design of technological and computing systems has implications for businesses, crime against those businesses, and ethical decision-making related to the creation of those designs.

Developed by the director of the Center for Cybersecurity, Education, and Research (Wu), this module begins by providing an overview of the way that the virtual world, physical world, and internet came together as one world, providing benefits in terms of improved artificial intelligence, automation, optimal performance, increased production, and efficiency. With these advantages, concerns about security also surface. Through an engineering lens, students are introduced to Supervisory Control and Data Acquisition (SCADA) Systems and Distributed Control Systems. The elements of SCADA (sensors and their specific types, communication systems, master terminal units, and remote terminal/telemetry units) are considered.

Once this foundation is created, the module turns to cyber vulnerabilities in engineering systems. Students learn that all devices are potential entry points for cyber attacks, and specific attention is given to three industrial cyber attacks gaining international attention (e.g., the Ukrainian power outage, the New York Dam attack, and Operation Ghoul). Whereas the IT module focused on policies and training as forms of security, the engineering module focused on weaknesses in the devices, systems, and networks. In doing so, the focus on vulnerabilities was conceptualized as stemming from the creation of systems and technologies that have security components integrated into the system (McDermott, 2019). As well, this module connects to the other modules by exploring the need to be able to identify and assess cyber vulnerabilities in the critical infrastructure (Ghiasi et al., 2020). Put simply, an engineering lens allows for the identification of vulnerabilities in computing and technological systems, thereby preventing or reducing harm to those systems and protecting individuals and businesses alike from criminal victimization or unethical behaviors.

To further generate interdisciplinary thinking, the module includes comparisons between the "engineering cyber world" and the "enterprise information technology" world. The balance between developing engineering tools that are both cost effective and effective in the business world is an important component when considering the connections between cybersecurity, technology, and society (Manson and Anderson, 2019). To shed light on the value of these strategies, engineering techniques for securing information (cryptography, cryptanalysis, and cryptology) are discussed. The module concludes with a detailed overview of engineering security design principles. After completing the module, students should be better equipped to describe the impact of cyber technology on engineering systems, identify vulnerabilities in engineering cyber system, and describe the design principles for securing cyber physical systems.

2.4 Module 4: Business and Cybersecurity

The fourth module explores cybersecurity within a business framework. In many ways, including a business module is based on the premise that cybersecurity is "a core business function that plays a critical role throughout business processes" (Li, 2015, p. 86). Certainly, a cyber incident can have a dramatic impact on business functions (Plachkinova and Maurer, 2019). Recognizing the core business function, the module begins by focusing on four areas: how businesses ensure computer systems and networks are safe, the types of cybersecurity businesses that exist or could be created, how businesses commit or are victims of cybercrime, and the employee's role in protecting business systems and networks. Building on themes provided in the earlier modules, the focus is on why businesses need to focus on cybersecurity and how they secure their systems and networks. Legal, ethical, financial, and psychological factors shaping the way businesses develop cybersecurity strategies are considered.

In discussing the role of businesses as criminals and victims of cybercrime, attention is given to the concept of white-collar cybercrime. Students are shown how white-collar crime is different from white-collar cybercrime: white-collar cybercrime tends to be more internationally focused, is defined as a national threat, has younger offenders, and has different underlying dynamics. Similarities identified between white-collar crime and white-collar cybercrime include the significant harm from both types of crime, the creation of specialized police units to address them, the problems defining both types of crime, and the setting where the crimes occur.

The Business and Cybersecurity module also explores the roles of customers, workers, and leaders in cybersecurity, with the bulk of attention given to the topic of "leadership and cybersecurity." Cybersecurity leadership principles are discussed, including "communication is vital," "lead by example," "awareness about risk matters," and several others. Similar to the way that information systems scholars have called efforts to bring entrepreneurship into the information systems curriculum (see Jones and Liu, 2017), integrated into this discussion is a principle focused on "opportunities for new businesses." This portion of the discussion includes an exercise where students are asked to use the letters of the word "C-Y-B-E-R-S-E-C-U-R-I-T-Y" to identify ways entrepreneurs might create cybersecurity businesses. Following this exercise, the discussion focuses on the many types of businesses created within the cyber operations, cyber insurance, cybersecurity consulting, cybersecurity products, and cybersecurity training domains. The module concludes by emphasizing the importance of collaboration in developing business-wide cybersecurity strategies. The main point stressed is that all employees are responsible for cybersecurity, but it is up to leadership to set the culture that demonstrates this responsibility.

2.5 Module 5: Computer Science and Cybersecurity

Implications in early cybersecurity literature suggested that cybercrime stemmed from situations where computers were used as tools to commit a crime and as targets of criminal behavior (Hale, 2002). The role of the computer, then, has historically been seen as central to cybersecurity incidents. Not surprisingly, computer scientists have taken a lead role in studying and teaching cybersecurity. In fact, early literature on the topic placed the onus of security education on the shoulders of computer scientists. One scholar, for example, suggested that "computer science educators bear the responsibility of cultivating a new generation of graduates who are aware of computer security related issues and are equipped with proper knowledge and skills to solve the problems" (Yang, 2001, p. 233). While some may believe that the topic of cybersecurity rests primarily within the discipline of computer science, the central theme of this course is that cybersecurity is an interdisciplinary field of study and not one that can be addressed solely in one discipline. To be sure, while cybersecurity is closely connected to computer science, it is actually a field that connects computer science to other disciplines (Jacob, Peters, and Yang, 2019).

The Computer Science and Cybersecurity module, like the engineering module, provides a slightly more technical orientation to cybersecurity. Developed by Wang (a computer scientist) and building on the concepts discussed in earlier modules, this module begins by providing a more technically-focused overview of the concepts of authentication, authorization, confidentiality, integrity, firewalls, and virtual private networks. The application of authentication within computing environments is considered. This module dives a little more deeply into authorization and provides a computing-focused overview of encryption types (symmetric encryption and asymmetric encryption). Such topics are, in many ways, analogous to the way that criminologists describe guardianship in the cybercrime literature (Leukfeldt and Yar, 2016).

Attention is also given to general types of attacks against computer systems. These include denial of service attacks, network attacks, and browser attacks. Specific types are also considered including theft support scams, crypto-jacking, port-scanning, spoofing, phishing, and buffer overflow attacks. Computing strategies to protect against these attacks are discussed including intrusion detection systems and firewalls. An introduction to the way firewalls work is provided. Taken together, the discussion provides an introduction to these activities through a technological lens. Connecting the topics to the other modules, particularly the last two modules, provides insight into the motives and behavioral explanations of the activities.

2.6 Module 6: Criminal Justice and Cybersecurity

The sixth module explores cybersecurity through a criminological and criminal justice paradigm. Attention is given to how criminal justice relates to cybersecurity, how cyber behavior comes to be labeled as criminal, specific forms of cybercrime, explanations for different types of cybercrime, and the way the justice system responds to these behaviors. Integrating micro- and macro-level perspectives, greater attention is given to human behavior in this module than the previous ones. The growth in cybercrime warrants considering these behaviors within a criminological perspective (Holt, 2016; Dupont, 2019). In addition, the notion of "cyber criminology" ("the study of causation of crimes that occur in the cyberspace and its impact in the physical space") is considered (Jaishankar, 2018, p. 2). To provide students a foundation in cybercrime and cyber criminology, the following areas are explored: conceptualizing cybercrime; explaining cyber offending and victimization; identifying guardianship activities; measuring victimization and offending; developing future employees; expanding the field of digital forensics; determining interventions; developing, researching, and understanding cyber law; seeking National Security Agency (NSA) designation; and conducting interdisciplinary research in criminal justice.

Unlike the more technical descriptions of similar behaviors provided in the previous modules, in this module a more behavioral and humanistic approach is followed. Such an approach is in line with the growing body of cybercrime research (Chang, 2019; Holt, Brewer, and Goldsmith, 2019). For each type of cybercrime, a number of areas are addressed, including the connection between other disciplines and the specific type of cybercrime. Risk factors for each type of cybercrime are also considered through an interdisciplinary lens.

The last part of the Criminal Justice and Cybersecurity module addresses the criminal justice system's response to cybercrime. An overview of the way the police, particularly federal law enforcement officers, respond to these behaviors includes a discussion of the types of agencies involved. The judicial response and sanctioning of cyber offenders includes examples of specific cybercrimes adjudicated in the courts. Focusing on the criminal justice processing of cybercrime cases helps to bring to life the overlap between criminal justice domains and the computing and technological domains (Borwell, Jansen, and Stol, 2018; Leukfeldt and Holt, 2019). This, in turn, shows the immediate and long-term consequences of various types of cyber incidents.

2.7 Module 7. Philosophy and Cybersecurity

Others have long recognized that ethics should be integrated into the information systems courses (Glass, 1994). At many universities, the strongest core of ethics content can be found in philosophy, a discipline that has been hailed as "the oldest of 'academic' subjects" (Niiniluoto, 1984). What this suggests is that all disciplines are grounded in philosophy. Philosophers note that when particular disciplines develop their own methods, concepts, and frames, they evolve out of philosophy into the newly formed discipline. In many ways, early aspects of cybersecurity are grounded in philosophical ideals. In fact, the connections between each of the other disciplines involved in the study of cybersecurity are, in some ways, held together by philosophical ideals. It was no accident that the course ended with this module – the instructors wanted students to learn about the fundamentals of cybersecurity and then begin to address philosophical and ethical questions that surface when cyber innovations create security and safety issues.

Throughout the readings for this module, which was developed more in line with how a philosophy course might be delivered, the instructor (Wittkower) developing this module incorporated voiceover notes in the readings to draw attention to the way that basic and fundamental questions about cybersecurity are best addressed through a philosophical lens. For instance, in one of the readings, Jonas (1979, p. 35) draws attention to the way that human nature impacts and is impacted by the behavior of mankind. In the part of the reading, the instructor offered the following voice over:

> In our particular area of concern, we might think about datafication or securitization. *Datafication* is the process of increasingly universal electronic storage of data about people and environments. We are only now starting to think about what the impacts of datafication might be in applications like healthcare datamining that can help predict disease but could lead to genetic discrimination or denial of health care coverage. Political use of data mining to strategically influence elections is another emerging, unforeseen concern about datafication, and big data analytics are also changing our advertising and economic systems. *Securitization* is the process of interpreting our actions and policies through a lens of security. As we use more data analytics in pursuit of security, we need to worry about ways that statistics may be used to infringe on civil liberties, marking people within particular demographics and communities as security risks, even though they haven't personally done anything to put anyone at risk.

In the same reading, the following voice over is included to encourage students to truly delve into important philosophical questions about technology and cybersecurity:

> This may be okay, of course. There isn't necessarily anything sacred about prior human nature. But if we are technologically changing human nature to fit our technological environment, we should at least think carefully about what we are doing. We should want to develop technology to support human flourishing, not to change humanity so that we can survive technological flourishing.

The statement has the potential to provoke deep and meaningful thinking among students who have already learned about the other cybersecurity topics through an interdisciplinary lens. Also considered in the readings for this module is Floridi's (2014) concept of hyper-history. This concept postulates that humanity entered the *historical* period when we began to use information technologies (like writing) to record events and to interpret reality; we left history and entered *hyperhistory* when information technologies became no longer a mere recording but a place where real events occur. Through the readings, students recognize that we are in an era where digital environments take on an independent reality, where, for example, someone who has never accessed the internet and has no phone or computer can nevertheless be attacked, harmed, and stolen from through digital communications alone. Students come to realize that information technologies require rethinking and renewed attention into many areas of our lives. Indeed, throughout the course, students will recognize that *hyperhistory* has altered virtually everything about our daily lives. The internet grew from something we accessed through our landline telephones to an Internet of Things that now connects our televisions, phones, refrigerators, automobiles, and door locks, among other personal items, to this vast network connected by electrons.

Questioning whether technology changes human nature should raise a wide range of emotions and thoughts in students. If who and what we are become defined by technology, then technology has an all-encompassing power over our very being. From this perspective, cybersecurity becomes a way to not only protect us, but as a possible tool or process to control us and potentially define who we are as human beings. It is this sort of thinking that is critical for cybersecurity students to engage in, whether they become cyber consumers, cyber professionals, business makers, or entrepreneurs. All too often, these questions come up after the fact. By including this critical module in the Cybersecurity, Technology, and Society class, students are encouraged to begin to think about these difficult questions at the beginning of their academic career, rather than down the road when the answers to those questions are beyond their control.

3. COURSE FORMAT AND ASSIGNMENTS

The course is taught both on-campus and online. Designed as a semester long course, typically two weeks are spent on each module with a week set aside for a midterm exam. Depending on the on-campus section, the course might meet two times a week or once a week. Five different faculty have taught the course, and each is able to design the delivery format in their preferred way as long as the general framework for the course remains intact.

The faculty decided that the students in the course would take two exams, complete a cybersecurity journal, produce an analytical paper, and develop an electronic portfolio. The exams are traditional types of exams developed by whichever faculty member instructs the class. The journal is central to the class. Each week students are asked to respond to a question related to the topic being reviewed. The questions are open-ended, with no right or wrong answer. Instead, students are asked to think deeply and critically about the questions and to provide their answers as homework assignments in an electronic portfolio (described below). The original set of journal questions we framed around the interdisciplinary theme of the course. Here is a summary of those questions:

- How does your major relate to cybersecurity technology?
- Select four other majors offered by ODU and explain how those majors relate to cybersecurity.
- Describe four ethical issues that arise when storing electronic information about individuals.
- Compare and contrast cybersecurity risks in the U.S. and another country.
- How do engineers make cyber networks safer?
- What role do engineers have in managing cyber risks?
- How has cyber technology created opportunities for workplace deviance?
- What are the costs and benefits of developing cybersecurity programs in businesses?
- How can you tell if your computer is safe?
- Describe three ways that computers have made the world safer and less safe.
- What is the overlap between criminal justice and cybercrime? How does this overlap relate to the other disciplines discussed in this class?
- How does cyber technology impact interactions between offenders and victims?
- How should we approach the development of cyber-policy and -infrastructure given the "short arm" of predictive knowledge?
- How should markets, businesses, groups, and individuals be regulated or limited differently in the face of diminishing state power and the intelligification and networking of the material world?
- How does cybersecurity relate to your future?

Students were asked to answer each question weekly, with each response required to be approximately 300 words. In the analytical paper, students are asked to build upon three of their journal entries and synthesize them in a way that demonstrates a full understanding of the connections between the different cybersecurity topics. The specific instructions included on the syllabus are the following:

> For this assignment you will produce a paper-length analysis of the social meaning and impact of cybersecurity-related technical systems. It'll be easier than it sounds. You'll produce a rough draft of most of the paper by combining three of the journal entry assignments you've already completed. After that, you'll edit and revise so that it reads smoothly, and then add a final section with a concluding analysis. In the end, you'll have a 1200+ word paper that draws from and draws together work that you've done throughout the course.

The electronic portfolio assignment is designed to hold all of these assignments together, figuratively and literally. Electronic portfolios are digital archives that allow students to organize their work and arrange their learning experiences in a way that presents a positive professional identity to potential employees. We elected to require electronic portfolios in our course for several reasons. First, a growing body of research shows that students experience "deep learning" when developing electronic portfolios (Barrett, 2001). Second, the cybersecurity program faculty decided to use electronic portfolios as one of its assessment tools. The literature demonstrates that electronic portfolios are superior to traditional hard copy portfolios when it comes to assessment (Yancey, 2001). Third, given the way that electronic portfolios are digital representations of self, inclusion of electronic portfolios in an interdisciplinary, general education, cybersecurity class provides an excellent opportunity to get the student to start thinking about their own digital identities. Fourth, and on a related point, there is growing evidence that employers want to "see" what students can do rather than just read a resume. A carefully constructed electronic portfolio can bring to life students' knowledge, skills, and abilities that employers seek. Moreover, given the increased focus on soft skills, like writing and communication, in cybersecurity jobs (Dawson and Thomson, 2018), an electronic portfolio allows students to demonstrate the full range of their skills, hard skills and soft skills alike. In some ways, for the introductory students, the portfolios introduce students to the need to integrate theoretical and practical skills which has been shown to be a critical part of information systems education (Hsu and Backhouse, 2002).

The students develop the electronic portfolio in the university's Word Press site and give the instructor access to the site for feedback and evaluation. The grade for the electronic portfolio is equivalent to an exam grade. Staff from the university's digital initiatives unit provide cybersecurity-specific electronic portfolio training both in-person and online, and an undergraduate cybersecurity mentor has been hired to help students develop their electronic portfolios. Faculty teaching other required cybersecurity courses have students use the electronic portfolio so that the full body of the student's work is available for assessment when students graduate.

As noted above, at the outset, the faculty agreed that we wanted to use open educational resources (OER) as the reading materials for our course. This decision was based on several factors. First, and perhaps most importantly, we were not able to locate a book that addressed cybersecurity in the way our course was designed. While scholars agree that cybersecurity is an interdisciplinary topic, the absence of an introductory book on the interdisciplinary nature of cybersecurity across business, engineering, information technology, computer science, computer engineering, and philosophy led us to conclude that open educational materials would be the best option.

A second reason we decided on OER materials is cost savings. Perhaps we could have found a couple of textbooks that, when combined together, addressed the topics we are covering. However, the growing cost of textbooks also influenced our decision to use open materials in our class. With the average textbook costing more than $90.00 (Hilton et al., 2014), we certainly didn't want to require multiple textbooks for the class. At ODU, more than 40 percent of our students are Pell-eligible. As a result, doing whatever we can to reduce the cost of an education made sense to us.

Third, a growing body of research is showing that students learn as much, if not more, from OER materials than they do from traditional textbooks (Weller et al., 2015; Colvard, Watson, and Park, 2018; Hilton, 2020). Part of the reason for this is that the reading materials are accessible by all students on the first day of class. With the traditional textbook model, some students may hold off on purchasing textbooks until they have enough money, and some even forgo purchasing their textbook altogether. These advantages of OER materials have led to more widespread use of the materials with new initiatives such as OER Commons available to help faculty locate a wide range of free course materials.

Finally, we preferred the open educational resource model because of the flexibility the model afforded. In particular, we are able to change readings easily between semesters or academic years. With a traditional textbook, no such luxury exists. The Appendix includes a sample of several of the open access readings initially included in the course. A quick review shows the breadth of the topics. It is important to note that we have, in fact, made some changes to the readings based on new materials becoming available and student and instructor feedback.

4. ASSESSMENT METHODS

The faculty have assessed the course in five different ways. First, ongoing assessment was initiated in the early stages of the course design progress. This initial assessment included syllabi review, review of readings, and development of a matrix showing how each module would align with general education learning outcomes. As part of the initial assessment, faculty expressed concern about the disjointedness of some of the modules. Discussing our concerns with an instructional designer, we decided to build transitional questions between each module in Blackboard to help students see the connections between the modules. While this may not have been a perfect solution, it was nonetheless a step towards helping to connect the modules.

Second, as part of a cybersecurity assessment summit held in May 2019 and led by our Office of Institutional Effectiveness and Assessment, the faculty came together to review all courses in the curricula. Course artifacts, with many of them coming for this new course, were reviewed to help us develop a program rubric that could be used to review the degree to which students were meeting learning outcomes. In addition, this initial assessment summit resulted in decisions to change the content needed for the electronic portfolio, and we used the feedback we received from the summit and students to further improve individual modules through an iterative process.

Third, in June 2020, we held a second cybersecurity assessment and used the rubric created the prior summer to review our artifacts. Sixteen faculty reviewed 92 artifacts from all required courses. During much of the summit, the faculty discussed how to best make sure that students are meeting the learning outcomes for the course, how to deliver the course as a general education course and a foundational course that prepares students for subsequent cybersecurity courses, the types of issues students and faculty face with using electronic portfolios, and whether the interdisciplinary framework is fully understood by the students.

Table 3 shows the results of the second summit. Bearing in mind that the summit focused on a variety of artifacts across multiple courses and assessed students at different stages of their academic development, the results were viewed as favorable. The results from the assessment showed that the vast majority of our students are meeting our stated learning outcomes. Though a sizable percentage were classified as "approaches standard" for select outcomes, because the artifacts came from introductory and upper-level courses and the summit focused on program-level outcomes rather than course-level outcomes, the results were viewed as positive. As a result of the second summit, a decision was made to more clearly define how the electronic portfolio is being used in the course and to require all faculty who teach the course to receive training in how to effectively integrate the electronic portfolio into the course with a particular focus on encouraging students to explain the connections between technology, cybersecurity, and society. In addition, because it appeared that the business module was not fully meeting our learning outcomes, a decision was made to revise the module.

Fourth, as part of our broader efforts to understand learning in the program, program faculty surveyed 47 students about their experiences with and perceptions about electronic portfolios. The results of the research have been examined in detail elsewhere (Payne et al., 2020). This line of research identified positive aspects of the electronic portfolios for cybersecurity students and opportunities for change. For instance, we found that two-thirds of the students thought the portfolio would help them get a job, and 83 percent indicated they would update their electronic portfolio in the future. In

Program Outcome – Student is able to:	Exceeds Standard	Meets Standard	Approaches Standard	Needs Attention
Integrate insights	14.20%	54.00%	23.00%	8.80%
Appropriately communicate complex to pics	13.50%	57.10%	24.60%	4.80%
Promptly apply interdisciplinary research process	6.40%	49.20%	38.90%	5.60%
Explain impact of technology	7.10%	46.00%	32.50%	14.20%
Understand the security landscape	8.70%	44.40%	33.30%	13.50%

Table 3. Program Assessment Results

addition, two-thirds of the students said it was easier to create the portfolio than they thought it would be. At the same time, 60 percent of the students said the electronic portfolio did not help them learn about topics in their major (Payne, Paredes, and Cross, 2020). However, a closer and qualitative look at the electronic portfolios done as part of the assessment summit described above suggests that the majority of students were learning from the electronic portfolio. As with many forms of active learning, students were learning, they just didn't realize that learning was occurring.

Finally, in April 2020, we surveyed by email all students who had taken the class since it was created. Students were asked to respond to the following four questions in a Qualtrics survey:

1. What did you like the most about the class?
2. What worked the best in helping you learn the material?
3. Please describe anything you didn't like about the class.
4. How would you describe the open-access materials used in the class?

In all, 23 students provided feedback to these questions. While a small percentage of the total who had taken the class, their feedback helped to assess the course. Table 4 includes some of the students' responses along with the themes that arose. The student survey revealed that students generally liked the course, including the breadth of course materials across various cybersecurity topics, the online component, the flexibility of allowing students to take open notes and absorb materials well, the interdisciplinary nature of the course, and the ability to foster critical thinking and interdisciplinary thoughts. Some students particularly indicated that this course sparked their interest toward cybersecurity, gave them an opportunity to explore the best cybersecurity career path fitting them, and provided information for various jobs in the cybersecurity field.

The student survey also showed that students appreciated the rich blending of various forms of teaching and course materials, including weekly quizzes, reading materials, audio, labs, guest speeches, visuals, group study, flash cards, etc. Students also praised the open-access materials of the course, indicating that they not only make it affordable to take the course, but also are very helpful and informative to help to understand cybersecurity.

Theme	Quotes from Students
Liked interdisciplinary content	I liked that the class was very interdisciplinary. It gave me and other students the chance to explore the various sides of cyber which really helped me analyze which cyber path I'm interested in most. This was genuinely the most enjoyable class that I took in the Cybersecurity program. Rather than being solely technical or step by step instructions on how to use a program, it fostered critical thinking and interdisciplinary thought with the social sciences and cyber security.
Liked the real world applications	I liked how the class went over a variety of ways Cybersecurity was related to the real world that I didn't know possible. I loved the mini hands-on assignments as well as the group projects. Most of all I like how the teacher gave real-life issues to help us get ready for what the real world looks likes. I enjoyed the application of the course material to real life scenarios and aspects to a career within the IT and Cybersecurity field. I also enjoyed the various guest speakers. This was actually my favorite part about that class because it provided people from these actual fields to give and detail their personal experiences. This provided us a sort of "intel" into what to expect upon entering these career fields ourselves and helps to ease nervousness or fear.
Cost savings from open access reading materials	The open-access materials were very informative and easy to understand. I'm especially grateful that these resources are free to anyone so they usually serve as a great reference tool for papers/research. I also find myself referring back to the open-access materials even after I finished the class. Textbooks are expensive and not always necessary, so having open-access was nice. I loved that I didn't have to spend a ton of money to take this class.
Hated it	(One student's response to "what did you like about the course"): Absolutely nothing, I failed the course twice because I had to continuously email BOTH professors that half of the questions on every quiz or test were WRONG. I even went higher up to the chair, and no one ever responded. So I failed out both times because I didn't believe I should be doing a professors job for them. Cost me thousands of dollars.

Table 4. Student Feedback about Cybersecurity, Technology, and Society

5. ENROLLMENT TRENDS

Cybersecurity, Technology, and Society has proven to be a popular course. In the first semester it was offered, 30 students enrolled in the class. By the Spring 2020 semester, 517 students had completed the course. Consistent with our expectations, the course attracted non-majors to the topic, with 169 non-majors taking the class. The most popular non-majors came from criminal justice (n = 51), leadership (n = 16), psychology (n = 13), computer sciences (n = 11), and information systems and technology (n = 9). In addition, the course attracted those who are often dissuaded from computing and technology courses. More than 31 percent of the students taking the course were females, which compares favorably to data from the National Center for Education Statistics suggesting that one-fifth of B.S. degrees earned in computer science in 2017-2018 were earned by females (NCES, no date). In addition, 55 percent of the students were underrepresented minorities, which included African American students (n = 200), Hispanic students (n = 34), and students of two or more races (n = 51). This, too, compares favorably to data from the NCES which shows that one-fifth of Bachelor's computer science degrees awarded in 2017-18 were earned by underrepresented minorities.

While courses by themselves aren't good predictors of retention, it is helpful to explore the major retention rate of students enrolled in general education courses. Among the 323 cyber majors taking the class, 80 percent returned the following semester with the same major. This seems to point to the success of keeping students enrolled and keeping them in the major.

6. RECOMMENDATIONS FOR DEVELOPING SIMILAR COURSES

Based on our experiences, we offer five recommendations for others developing similar courses. First, we encourage faculty to draw on the strengths of interdisciplinary efforts when developing similar courses. Among others, these strengths include the fact that such an approach reflects the real world where disciplinary boundaries do not define human behavior, with recent workforce changes potentially making it even more important to promote an interdisciplinary approach (Woodside et al., 2020). As well, interdisciplinary efforts bring ideas together in ways that integrate multiple perspectives to identify solutions to various problems and help students improve critical thinking capabilities (Carmichael, Dellner, and Szostak, 2017). Repko, Szostak, and Buchberger (2014) offer the metaphor of a fruit salad and a smoothie. A fruit salad is multidisciplinary in that the fruit (e.g., disciplines) creating the salad is still recognizable. In contrast, drawing on the work of Nissani (1995), the authors note that with a smoothie, the original fruit (e.g., discipline) cannot be distinguished from its original form. Cybersecurity solutions must take into account all perspectives – human, technical, legal, political, ethical, scientific, and economic alike.

Second, it is important that faculty "practice what they preach" when it comes to interdisciplinary cybersecurity efforts. In this context, what this means is that such courses should not be "owned" by a specific department or a specific faculty member. Doing so would send an inadvertent message that the course is disciplinary-based rather than interdisciplinary in nature. In our case, in the past year alone, we had four different faculty teach the class with backgrounds from four different disciplines: international studies, engineering, information technology, and computer science.

Third, faculty and students taking interdisciplinary general education courses are encouraged to "think small, not big." Such a recommendation may be counterintuitive. Stakeholders must bear in mind that it's one class, not an entire program. It is equally important to remember that cybersecurity is a broad and evolving discipline (Cabaj et al., 2018). With so much information available that relates to the topic, the challenge is not deciding what to cover in such a course. Instead, the challenge becomes deciding what not to cover. For us, focusing on the learning outcomes and using a "learner centered" paradigm helped us decide which material to include. Students should not be expected to become master cybersecurity experts from taking an introductory interdisciplinary general education class. While depth in a particular area is needed for most cybersecurity careers (Manson and Pike, 2014), it is unrealistic to assume that depth can be achieved in an introductory course.

Fourth, faculty are encouraged to explore the different ways that information security courses might be integrated into their university's general education curriculum. It is important to note that computing and information technology general education classes can focus on more than technology, computing, and quantitative reasoning (Tartaro, Healy, and Treu, 2016; Healy and Greenville, 2018; Farrell and Robertson, 2019). Using our experiences in developing a general education technology class on cybersecurity, the cybersecurity program is now developing a general education social science class on cybersecurity. This future course will embrace the interdisciplinary ideals highlighted above and focus on how cybersecurity can be understood through a social science lens.

Finally, faculty developing similar efforts are encouraged to not reinvent the wheel. On the one hand, open education resources are growing in popularity and can be quite helpful. Some class materials are also available to the public. In fact, while our enrolled students access their course materials in the course through Blackboard, we have made the course available to the public on our Center's website. Materials are available at https://sites.wp.odu.edu/cyse-200/. Modules can be used in part or in their entirety by others. We encourage those seeking materials for their introductory cybersecurity classes to visit the site. As well, others are encouraged to make the course materials public to help generate access to interdisciplinary information that can be used to change the world.

7. ACKNOWLEDGEMENTS

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 http://cyberinitiative.org.

8. REFERENCES

Alvin, C. (2019). Student Generation of an Optimal Decision Procedure Using Guess Who? *Journal of Computing Sciences in Colleges*, 34(6), 26-34.

Anduiza, E., Perea, E. A., Jensen, M. J., & Jorba, L. (eds.). (2012). *Digital Media and Political Engagement Worldwide: A Comparative Study*. Cambridge, U.K.: Cambridge University Press.

Atkinson, R. D. & Mayo, M. (2010). *Refueling the US Innovation Economy: Fresh Approaches to Science, Technology, Engineering and Mathematics (STEM) Education.* Washington, D.C.: Information Technology and Innovation Foundation.

Barrett, H. (2001). ePortfolios: Digital Stories of Deep Learning. *Work,* 1(11/9), 89.

Bimber, B., Cunill, M. C., Copeland, L., & Gibson, R. (2015). Digital Media and Political Participation. *Social Science Computer Review*, 33(1), 21-42.

Borwell, J., Jansen, J., & Stol, W. (2018). Human Factors Leading to Online Fraud Victimisation: Literature Review and Exploring the Role of Personality Traits. In J. McAlaney, L. A. Frumkin, & V. Benson (eds.), *Psychological and Behavioral Examinations in Cyber Security* (pp. 26-45). Hershey, Pennsylvania: IGI Global.

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity Education. *Computers & Security,* 75, 24-35.

Carmichael, T., Dellner, J,. & Szostak, R. (2017). Report from the Field: Interdisciplinary General Education. *Issues in Interdisciplinary Studies*, 35, 248-258.

Case, T., Dick, G., Granger, M. J., & Akbulut, A. Y. (2019). Teaching Information Systems in the Age of Digital Disruption. *Journal of Information Systems Education*, 30(4), 287–297.

Chang, L. Y. C. (2019). Criminological Perspectives on Cybercrime: Risk, Routine Activity, and Cybercrime. In *Research Handbook on Transnational Crime*. Cheltanham, U.K.: Edward Elgar Publishing.

Chesnes, M. & Jin, G. Z. (2019). Direct-to-Consumer Advertising and Online Search. *Information Economics and Policy*, 46, 1-22.

Colvard, N. B., Watson, C. E., & Park, H. (2018). The Impact of Open Educational Resources on Various Student Success Metrics. *International Journal of Teaching and Learning in Higher Education*, 30(2), 262-276.

Cyberseek.org. (2020). Hack the Gap. Retrieved December 28, 2020, from https://www.cyberseek.org/.

Dawson, J. & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology,* 9(744).

Dupont, B. (2019). Enhancing the Effectiveness of Cybercrime Prevention through Policy Monitoring. *Journal of Crime and Justice*, 42(5), 500-515.

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.

Farrell, K. & Robertson, J. (2019). Interdisciplinary Data Education: Teaching Primary and Secondary Learners How to be Data Citizens. In *Proceedings of the 14th Workshop in Primary and Secondary Computing Education*, 1-2.

Fisher, N. (2019). How Much Time Americans Spend in Front of Screens Will Terrify You. *Forbes*. Retrieved December 29, 2020, from https://www.forbes.com/sites/nicolefisher/2019/01/24/how-much-time-americans-spend-in-front-of-screens-will-terrify-you/#7dc3b5831c67.

Floridi, L. (2014). *The Fourth Revolution*. Oxford, U.K.: Oxford University Press.

Fulton, E., Lawrence, C., & Clouse, S. (2013). White Hats Chasing Black Hats: Careers in IT and the Skills Required to Get There. *Journal of Information Systems Education*, 24(1), 75-80.

Glass, R. (1994). Integrating Ethics into Information Systems Courses: A Multi-Method Approach Based on Role Playing. *Journal of Information Systems Education*, 6(4), 188-191.

Ghiasi, M., Dehghani, M., Niknam, T., & Kavousi-Fard, A. (2020). Investigating Overall Structure of Cyber-Attacks on Smart-Grid Control Systems to Improve Cyber Resilience in Power System. *IEEE Smart Grid Newsletter*.

Goh, S. H., Di Gangi, P. M., & Gunnells, K. (2020). Applying Team-Based Learning in Online Introductory Information Systems Courses. *Journal of Information Systems Education*, 31(1), 1-11.

Goonewardene, A. U., Offutt, C. A., Whitling, J., & Woodhouse, D. (2016). An Interdisciplinary Approach to Success for Underrepresented Students in STEM. *Journal of College Science Teaching*, 45(4), 59-67.

Hale, C. (2002). Cybercrime: Facts & Figures Concerning this Global Dilemma. *Crime and Justice International*, 18(65), 5-6.

Hallam, C. & Zanella, G. (2017). Online Self-Disclosure: The Privacy Paradox Explained as a Temporally Discounted Balance Between Concerns and Rewards. *Computers in Human Behavior*, 68, 217-227.

Hargittai, E. & Marwick, A. (2016). "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication*, 10, 3737-3757.

Hefner, P. (2003). *Technology and Human Becoming.* New York, New York: Fortress Press.

Healy, C. A. & Greenville, S. C. (2018). Teaching the Historical Context of Computing. *Journal of Computing Sciences in Colleges*, 33(5), 40-45.

Hilton, J. L., Robinson, T. J., Wiley, D., & Ackerman, J. D. (2014). Cost-Savings Achieved in Two Semesters through the Adoption of Open Educational Resources. *International Review of Research in Open and Distributed Learning*, 15(2), 67-84.

Hilton, J. (2020). Open Educational Resources, Student Efficacy, and User Perceptions: A Synthesis of Research Published Between 2015 and 2018. *Educational Technology Research and Development*, 68**,** 853–876

Hoffman, L. J., Burley, D., & Toregas, C. (2011). Thinking Across Stovepipes: Using a Holistic Development Strategy to Build the Cybersecurity Workforce. *IEEE Security and Privacy*, 1(13).

Holt, T. J. (ed.). (2016). *Cybercrime through an Interdisciplinary Lens*. New York, New York: Taylor & Francis.

Holt, T. J., Brewer, R., & Goldsmith, A. (2019). Digital Drift and the "Sense of Injustice." *Deviant Behavior*, 40(9), 1144-1156.

Hsu, C. & Backhouse, J. (2002). Information Systems Security Education: Redressing the Balance of Theory and Practice. *Journal of Information Systems Education*, 13(3), 211-218.

Jacob, J., Peters, M., & Yang, T. A. (2019). Interdisciplinary Cybersecurity: Rethinking the Approach and the Process. In *National Cyber Summit* (pp. 61-74), Switzerland: Springer.

Jaishankar, K. (2018). Cyber Criminology as an Academic Discipline: History, Contribution and Impact. *International Journal of Cyber Criminology*, 12(1), 1-8.

Jonas, H. (1979). Toward a Philosophy of Technology. *Hastings Center Report*, 34-43.

Jones, C. G. & Liu, D. (2017). Approaches to Incorporating Entrepreneurship into the Information Systems Curriculum. *Journal of Information Systems Education*, 28(1), 43-58.

Kim, H. S., Cho, K. M., & Kim, M. (2019). Information-Sharing Behaviors among Sports Fans using #hashtags. *Communication & Sport*.

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education*, 28(2), 101-114.

Konstantinou, C. & Mohanty, S. P. (2020). Cybersecurity for the Smart Grid. *IEEE Computer*, 53(5), 10-12.

Kostyuk, N. & Wayne, C. (2020). The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public. *Journal of Global Security Studies*, 6(2).

Krug, K. S., Dickson, K. W., Lessiter, J. A., & Vassar, J. S. (2016). Student Preference Rates for Predominately Online, Compressed, or Traditionally Taught University Courses. *Innovative Higher Education*, 41(3), 255-267.

LeBourgeois, M. K., Hale, L., Chang, A. M., Akacem, L. D., Montgomery-Downs, H. E., & Buxton, O. M. (2017). Digital Media and Sleep in Childhood and Adolescence. *Pediatrics,* 140, S92-S96.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information Security Awareness and Behavior: A Theory-Based Literature Review. *Management Research Review*, 37, 1049-1092.

Lee, Y. G., Stringer, D. Y., & Du, J. (2017). What Determines Students' Preference of Online to F2F Class? *Business Education Innovation Journal*, 9(2), 97-102.

Leukfeldt, R. & Holt, T. J. (eds.). (2019). *The Human Factor of Cybercrime*. New York, New York: Routledge.

Leukfeldt, E. R. & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime. *Deviant Behavior*, 37(3), 263-280.

Li, C. (2015). Penetration Testing Curriculum Development in Practice. *Journal of Information Technology Education: Innovations in Practice*, 14(1), 85-99.

Logan, P. Y. (2020). Crafting an Undergraduate Information Security Emphasis within Information Technology. *Journal of Information Systems Education*, 13(3), 177-182.

Manson, S. & Anderson, D. (2019). Cybersecurity for Protection and Control Systems. *IEEE Industry Applications Magazine*, 25(4), 14-23.

Manson, D. & Pike, R. (2014). The Case for Depth in Cybersecurity Education. *ACM Inroads,* 5(1), 47-52.

McDermott, T. A. (2019). A Rigorous System Engineering Process for Resilient Cyber-physical Systems Design. In *2019 International Symposium on Systems Engineering (ISSE)*, 1-8.

Moll, E. (2020). Citizen Epistemology and Interdisciplinary, Inclusive Curriculum. *The Journal of General Education*, 68(1-2), 19-31.

Mountrouidou, X., Li, X., & Burke, Q. (2018). Cybersecurity in Liberal Arts General Education Curriculum. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, 182-187.

National Center for Education Statistics. (ND). *Digest of Education Statistics.* Retrieved December 29, 2020, from https://nces.ed.gov/programs/digest/2019menu_tables.asp.

Niiniluoto, I. (1984). How is Philosophy Possible as a Science? In *Is Science Progressive?* Switzerland: Springer, 10-17.

Nissani, M. (1995). Fruits, Salads, and Smoothies: A Working Definition of Interdisciplinarity. *The Journal of Educational Thought*, 29, 121-128.

Nodeland, B., Belshaw, S., & Saber, M. (2019). Teaching Cybersecurity to Criminal Justice Majors. *Journal of Criminal Justice Education*, 30(1), 71-90.

O'Hallarn, B., Shapiro, S. L., Wittkower, D. E., Ridinger, L., & Hambrick, M. E. (2019). A Model for the Generation of Public Sphere-Like Activity in Sport-Themed Twitter Hashtags. *Sport Management Review,* 22(3), 407-418.

Payne, B. K., Mayes, N., Paredes, T., Smith, E., Wu, H., & Xin, C. (2020). Applying High Impact Practices in an Interdisciplinary Cybersecurity Program. *Journal of Cybersecurity Education, Research, and Practice*, 2020(2), 4.

Payne, B. K., Paredes, T., & Cross, B. (2020). Student Perceptions about the Production of Electronic Portfolios: Technology, Process, and Showcase Insights. *Education*, 141(2), 67-78.

Plachkinova, M. & Maurer, C. (2019). Security Breach at Target. *Journal of Information Systems Education*, 29(1), 11-20.

Rege, A., Williams, K., & Mendlein, A. (2019). An Experiential Learning Cybersecurity Project for Multiple STEM Undergraduates. In *2019 IEEE Integrated STEM Education Conference (ISEC)*, 169-176.

Repko, A. F., Szostak, R., & Buchberger, M. P. (2014). *Introduction to Interdisciplinary Studies.* Thousand Oaks, California: Sage Publications.

Rhoten, D. & Pfirman, S. (2007). Women in Interdisciplinary Science: Exploring Preferences and Consequences. *Research Policy*, 36(1), 56-75.

Scott, H. & Woods, H. C. (2019). Understanding Links Between Social Media Use, Sleep and Mental Health. *Current Sleep Medicine Reports*, 5(3), 141-149.

Shoemaker, D. & Kohnke, A. (2016). Cyber Education and the Emerging Profession of Cybersecurity. *The EDP Audit, Control, and Security Newsletter,* 54(5), 12-16.

Stockman, M. (2013). Infusing Social Science into Cybersecurity Education. In *Proceedings of the 14th Annual ACM SIGITE Conference on Information Technology Education*, 121-124.

U.S. Department of Commerce (2020). Quarterly Retail e-commerce Sales. Retrieved April 1, 2021, from https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

Tartaro, A., Healy, C., & Treu, K. (2016). Computer Science in General Education: Beyond Quantitative Reasoning. *Journal of Computing Sciences in Colleges*, 32(2), 177-184.

Topi, H. (2019). Reflections on the Current State and Future of Information Systems Education. *Journal of Information Systems Education*, 30(1), 1-9.

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.

Vasileiou, I. & Furnell, S. (2019). *Cybersecurity Education for Awareness and Compliance.* Hershey, Pennsylvania: IGI Global.

Vicente, K. (2010). *The Human Factor: Revolutionizing the Way we Live with Technology*. Vintage.

Wang, P. & D'Cruze, H. (2019). Cybersecurity Certification: Certified Information Systems Security Professional (CISSP). In *16th International Conference on Information Technology-New Generations (ITNG 2019)*, 69-75.

Weiss, R., Mountrouidou, X., Watson, S., Mache, J., Hawthorne, E., & Chattopadhyay, A. (2020). Cybersecurity Across All Disciplines in 2020. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, 1404-1404.

Weller, M., De los Arcos, B., Farrow, R., Pitt, B., & McAndrew, P. (2015). The Impact of OER on Teaching and Learning Practice. *Open Praxis*, 7(4), 351-361.

Whitman, M. E. & Mattord, H. J. (2011). *Principles of Information Security*. Boston, Massachusetts: Cengage.

Wittkower, D. (2020). Privacy as Care. In H. Wiltse (ed.), *Relating to Things: Design, Technology and the Artificial*. New York, New York: Bloomsbury, 15-29.

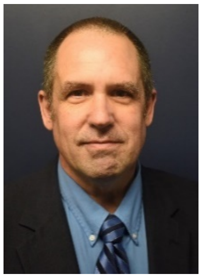
Woodside, J. M., Augustine, F. K., Jr., Chambers, V., & Mendoza, M. (2020). Integrative Learning and Interdisciplinary Information Systems Curriculum Development in Accounting Analytics. *Journal of Information Systems Education,* 31(2), 147-156.

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the Weakest Links in the Weakest Link. *Computers in Human Behavior,* 84*,* 375-382.

Yang, T. A. (2001). Computer Security and Impact on Computer Science Education. In *Proceedings of the Sixth Annual CCSC Northeastern Conference on the Journal of Computing in Small Colleges*, 233-246.

Yancey, K. B. (2001). Digitized Student Portfolios. In B. Cambridge (ed.), *Electronic Portfolios: Emerging Practices in Student, Faculty, and Institutional Learning*. Washington, D.C.: American Association for Higher Education, 15-30.

AUTHOR BIOGRAPHIES



Brian K. Payne is vice provost for academic affairs and professor of sociology and criminal justice at Old Dominion University. He received his Ph.D. in criminology from Indiana University of Pennsylvania. He serves as the director of the Coastal Virginia Center for Cyber Innovation, a regional node of the Commonwealth Cyber Initiative and has been PI or co-PI on more than $7 million in federal and state grants. His research explores white-collar crime, cybercrime, and the overlap between the two types of crime. Payne is the author or co-author of more than 160 scholarly journal articles and 8 textbooks.

Wu He is an associate professor of information technology in the Department of Information Technology & Decision Sciences at Old Dominion University. He has been the PI or co-PI of grants totaling over $3M funded by the National Science Foundation and other federal agencies. He is also the editor-in-chief of *Information Discovery & Delivery* and associate editor of *Behavior & Information Technology*. He has served as a Program Director at the National Science Foundation and has managed numerous education-related proposals and awards in areas of data science, computer science, cybersecurity, artificial intelligence, robotics, quantum information science, and information technologies.

Cong Wang joined the Computer Science Department of Old Dominion University as an assistant professor in 2017. He is also affiliated with the School of Cybersecurity. Cong's research focuses on exploring algorithmic solutions to address security and privacy challenges in mobile/cloud computing, IoT, machine learning, and systems. He received his Ph.D. from Stony Brook University in 2016, a B.Eng. in information engineering from the Chinese University of Hong Kong in 2008, and a M.S. in electrical engineering from Columbia University in 2009. He is the recipient of a COVA-CCI Cybersecurity Research and Innovation Award in 2020, ODU Cheng Fund for Innovative Research in 2020, and IEEE PERCOM Mark Weiser Best Paper Award in 2018. Prior joining ODU, he worked in a research position in industry.

D.E. Wittkower is an associate professor and chair of the Department of Philosophy and Religious Studies at Old Dominion University, where he teaches on philosophy of technology, information ethics, information literacy, and cybersecurity. His research focuses on and branches out from the intersection of phenomenology of technology and feminist ethics of care. He has published work on topics including discrimination in design, informational economies of care, self and self-performance on Facebook, friendship online, the function and value of boredom on SNS, the role of the cute in digital culture, the phenomenology of audiobooks, the Occupy movement, ethics of care and employee loyalty, exploitation and community in crowdfunding, and the crisis in copyright. Current research focuses on data justice and anti-discriminatory design, with emphasis on race and disability.

Hongyi Wu is the Batten Chair of Cybersecurity and the Director of the School of Cybersecurity at Old Dominion University. He is also a professor in the Department of Electrical and Computer Engineering and holds a joint appointment in the Department of Computer Science. Before joining ODU, he was an Alfred and Helen Lamson Professor at the Center for Advanced Computer Studies (CACS), University of Louisiana at Lafayette. He received his Ph.D. in computer science from the State University of New York (SUNY) at Buffalo. His research focuses on networked and intelligent cyber-physical systems for security, safety, and emergency management applications. He chaired several conferences such as IEEE Infocom 2020, IEEE WoWMoM 2016, and IEEE Globecom Wireless Communication Symposium 2015. He also served on the editorial board of several journals including *IEEE Transactions on Mobile Computing*, *IEEE Transactions on Parallel and Distributed Systems*, and *IEEE Internet of Things Journal*. He received an NSF CAREER Award in 2004, a UL Lafayette Distinguished Professor Award in 2011, and an IEEE Percom Mark Weiser Best Paper Award in 2018. He is a Fellow of IEEE.

APPENDIX

Sample OER Materials Used in Course

Bourgeois, D. T. (2014). *Information Systems Security.* Washington D.C.: Saylor Academy.

Brooks, S., Brooks, S., Garcia, M., Lefkovitz, N., Lightman, S., & Nadeau, E. (2017). *An Introduction to Privacy Engineering and Risk Management in Federal Systems*. Washington D.C.: U.S. Department of Commerce, National Institute of Standards and Technology.

Choong, Y. Y., Theofanos, M., & Liu, H. K. (2014). *United States Federal Employees' Password Management Behaviors: A Department of Commerce Case Study*. Washington D.C.: U.S. Department of Commerce, National Institute of Standards and Technology.

Cichonski, P., Millar, T., Grance, T., Scarfone, K. (2012). *Computer Security Incident Handling Guide.* Washington D.C.: U.S. Department of Commerce, National Institute of Standards and Technology.

Collins, J. D., Sainato, V. A., & Khey, D. N. (2011). Organizational data breaches 2005-2010: Applying SCP to the healthcare and education sectors. *International Journal of Cyber Criminology*, *5*(1), 794-810.

Federal Communications Commission. (2013). *Cybersecurity for Small Business.* Retrieved from https://www.sbir.gov/tutorials/cyber-security/.

Floridi, L. (2015). *The Onlife Manifesto.* Switzerland: Springer-Verlag GmbH. Retrieved from https://link.springer.com/book/10.1007%2F978-3-319-04093-6

Hazelwood, S. D., & Koon-Magnin, S. (2013). Cyber Stalking and Cyber Harassment Legislation in the United States. *International Journal of Cyber Criminology*, 7(2), 155-168.

Holt, T. J., & Bolden, M. S. (2014). Technological Skills of White supremacists in an Online Forum: A Qualitative Examination. *International Journal of Cyber Criminology*, *8*(2), 79-93.

ICF International (2016). *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats.* Washington D.C.: U.S. Department of Energy.

Kigerl, A. (2016). Cyber Crime Nation Typologies: K-Means Clustering of Countries Based on Cyber Crime Rates. *International Journal of Cyber Criminology*, 10(2), 147-169.

Payne, B. K., Hawkins, B., & Xin, C. (2019). Using Labeling Theory as a Guide to Examine the Patterns, Characteristics, and Sanctions Given to Cybercrimes. *American Journal of Criminal Justice*, 44(2), 230-247.

Payne, B. K. (2018). White-collar Cybercrime: White-collar Crime, Cybercrime, or Both. *Criminology, Criminal Justice, Law, & Society*, 19, 16-33.

Souppaya, M., & Scarfone, K. (2013). Guidelines for Managing the Security of Mobile Devices in the Enterprise. U.S. Department of Commerce: Washington D.C.

Toth, P. R., & Paulsen, C. (2016). Small Business Information Security: The Fundamentals. U.S. Department of Commerce: Washington D.C.

Van Ommeren, E., Borrett M., & Kuivenhoven, M. (2014). *Staying Ahead in the Cyber Security Game*. New York: Sogeti.

Information Systems & Computing
Academic Professionals

EDSIG
Serving Information Systems Educators

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 2574-3872