2022

Digital Educational Modules Development For The Career and Technical Cybersecurity Pathways During the COVID-19 Pandemic

Vukica Jovanović
Old Dominion University, v2jovano@odu.edu

Murat Kuzlu
Old Dominion University, mkuzlu@odu.edu

Otilia Popescu
Old Dominion University, opopescu@odu.edu

Petros Katsioloudis
Old Dominion University, pkatsiol@odu.edu

Linda Vahala
Old Dominion University, lvahala@odu.edu

See next page for additional authors

Original Publication Citation
Jovanovic, V., Kuzlu, M., Popescu, O., Katsioloudis, P., Vahala, L., Wu, M., Marshall, D., Crespo, M., & Addison, M. (2022). Digital educational modules development for the career and technical cybersecurity pathways during the COVID-19 pandemic. *Technology Interface International Journal*, *22*(2), 22-34. https://tiij.org/issues/issues/spring2022/X__TIIJ%20spring%202022%20v22%20n2.pdf#page=24

Authors

Vukica Jovanović, Murat Kuzlu, Otilia Popescu, Petros Katsioloudis, Linda Vahala, Michael Wu, Deborah Marshall, Michael Crespo, and Mary Addison

Digital Educational Modules Development for the Career and Technical Cybersecurity Pathways during the COVID-19 Pandemic

Vukica Jovanovic, Old Dominion University; Murat Kuzlu, Old Dominion University; Otilia Popescu, Old Dominion University; Petros Katsioloudis, Old Dominion University; Linda Vahala, Old Dominion University; Michael Wu, Old Dominion University; Deborah Marshall, Norfolk Public Schools; Michael Crespo, Norfolk Public Schools; Mary Addison, Old Dominion University

Abstract

Virtual learning has been used now for several decades, but it has never had a bigger impact on student learning than in the era of the COVID-19 pandemic. Universities and schools faced shutdowns all around the world, and teachers had to adapt rapidly to online mode of instruction. Many educators were faced with a triage approach with no previous experience in distance learning, a lack of resources for professional development, and already existing shortages of current educational modules that could assist them in their day-to-day jobs. This gap was especially evident in areas such as career and technical education (CTE) in which there was a gap in the training and educational materials available for K-12 teachers in emerging technology fields such as computer science and cybersecurity.

These problems are related to various issues, such as the lack of teacher preparation, constant changes in technology, curriculum and educational framework developments led by the various institutions dictating the nature of education, and moreover, the vast growth in the demand for such instruction, which presents challenges in meeting those growing demands. In this paper, the authors present one curriculum development effort for CTE high school programs focused on computer science and cybersecurity via a grant by the Perkins Innovation Project funded by the U.S. Department of Education and supported by engineering technology, electrical engineering, and industrial technology educators.

Introduction

The main problem that researchers are trying to solve is the lack of current educational resources available in the area of CTE cybersecurity for high school teachers that are current in their skillsets (according to the industry need), based on Virginia Department of Education competencies. The area of cybersecurity is facing rapid growth and currently there is a lack of sufficient materials available for CTE teachers to teach all cybersecurity courses in the pathway. The research question for this study was:

Would a partnership between the CTE department, university, and industry improve hands-on CTE cybersecurity educational modules that can be easily integrated into virtual or in-person high school curricula?

Hypothesis: *Online access to the hands-on CTE cybersecurity educational modules accessible to CTE cybersecurity teachers will lead to a better understanding of cybersecurity careers and pathways.*

Research Objective: *Develop, assess, and improve hands-on CTE cybersecurity educational modules that can be easily integrated into a high school curriculum.*

Currently, there are a plethora of resources and educational modules being developed nationwide for various math and science topics that are funded by various federal agencies. Many of these modules are scattered and they are not integrated into specific pathways, or into the multiple classes, at the state level. The main research gap is present in educational programming and support available for the area of career and technical education, which is mainly supported by the U.S. Department of Education Perkins 5 Act funding. Even CTE teachers' salaries are funded differently than other high school teachers, and each year school districts have to make sure that they apply for these funds and that these funds are available for CTE pathways such as cybersecurity.

However, there is no related work that was documented in terms of engaging CTE departments, university, and industry on one such curriculum development project through an integrated approach. Work on this current study was done with the support of the CTE department from a local Norfolk Public School district. Modules were then improved, following feedback from an industrial advisory board and with the help of instructional developers. Modules were distributed to all cybersecurity CTE teachers in the Commonwealth of Virginia by Judith Sams, Specialist, Business & Information Technology and Related Clusters - Virginia Department of Education.

The Impact of COVID-19 On CTE Teachers

The COVID-19 pandemic has had an enormous impact on work, entertainment, travel, and education (Radha, Mahalakshmi, Sathis Kumar, & Saravanakumar, 2020). In addition, recommended standards, such as social distancing and physical distancing, by the World Health Organization (2019) increased its impact on lives even more (Aliyyah, Rachmadtullah, Samsudin, Syaodih, Nurtanto & Tambunan, 2020). These regulations were also extended by governments and local administrations to include working from home, homeschooling, virtual learning, stay-at-home orders, etc. Due to COVID-19, many K-12 students in the U.S. were also missing access to face-to-face education. The general public shared a common concern about student achievement, as well as the possible negative effects on widening the gap between high- and low-achieving students. In a study by Aliyyah et al. (2020), the authors investigated the impacts of COVID-19 on student achievement and what it may mean for educators.

The results indicated that: 1) students might be substantially behind, especially in mathematics; 2) students are likely to enter school with more variability in their academic skills than under normal circumstances; and, 3) under normal circumstances, students who lose the most during the summer tend to gain the most when back in school, but this may not hold during COVID-19 instruction time. Multiple states in the U.S. have developed a web platform and related websites to share the most up-to-date information and resources with teachers and communities. For example, the Virginia Department of Education (VDOE) guidance for the 2020-2021 school year, including Virginia's return to school plan, school reopening frequently asked questions, and Virginia's phase guidance for reopening schools (Aliyyah et al., 2020). Universities and school districts developed web pages that would address special guidelines related to online learning and to different support materials needed for online instruction.

The pervasiveness of the COVID-19 pandemic has significantly increased since it started, making it difficult to return to everyday life. The long-term impacts of the COVID-19 pandemic are still uncertain. One of those impacts is related to the significant way it affected the education process. Students would be the most affected group, due to a lack of face-to-face education during COVID-19. The lockdowns in response to COVID-19 have interrupted conventional education in most countries, with the majority lasting at least ten weeks (Aliyyah et al., 2020). However, students should still gain enough knowledge, skills, and attitudes, as well as values and social interaction that would be otherwise provided by the educational systems to sufficiently drive subsequent generations.

According to a report released by UNESCO, 132 countries worldwide have been implementing nationwide closures due to the COVID-19 pandemic, which affected 1,048,817,181 students (i.e., 59.9%) of all enrolled students at the pre-primary, primary, lower-secondary, and upper-secondary levels of education, as well as in higher education (Aliyyah et al., 2020). Various studies are now trying to understand the impacts of student learning, while educators have been forced to determine how to provide distance learning even though they did not have previous experience or much support (Hoffman & Miller, 2020).

The COVID-19 pandemic has severely impacted educational systems from elementary schools, middle schools, and high schools, and post-secondary institutions. While some universities quickly responded and replaced face-to-face lectures with virtual learning and educational tools, other schools had difficulties in terms of adaptation due to a lack of teachers' and students' experience, resources, and supportive environments. From this current study, the authors present the development of digital educational modules for virtual learning in the computer science and cybersecurity pathway in high schools during the COVID-19 pandemic. These modules were developed for high school CTE teachers by a team of undergraduate students, graduate students, and engineering college professors with the help of educational professionals. All modules were revised by the high school teacher practitioners, reviewed by industry practitioners, and finalized by a professional instructional designer.

Learning over Distance Education

Virtual learning is defined broadly in many ways. Although those learning forms look similar, they are different in terms of the aspects of learning and teaching. They vary greatly in terms of adequate technical support and available facilities, especially during the COVID-19 pandemic. Many of the professors, teachers, and students have to participate in the teaching and learning process in virtual environments, while facing issues with internet connectivity, up-to-date devices, noise at the places from where they were participating, and other issues that were not encountered previously in well-established distance learning programs.

e-Learning refers to the use of electronic technologies, such as the world wide web, an intranet, or other multimedia materials, for learning and teaching, which can be conducted by means of electronic media with or without the use of the internet. It is also considered a type of online learning and has been widely used for the last decade with advances in technology and changes in society. There are a variety of e-learning forms—standalone courses, learning games and simulations, mobile learning, social learning, and virtual classroom courses (Horton, 2011). e-Learning has been used for a relatively long time. However, it is still considered immature, due to a lack of organizational aspects of teaching and only focusing on supporting learning. This causes students to become de-individualized and demoted to a non-critical, homogenous users. To deal with these drawbacks, various researchers have suggested creating individual e-learning materials using flexible, multidimensional data models and individual content in order to improve the success of e-learning systems (Tavangarian, Leypold, Nölting, Röser & Voigt, 2004).

Web-based learning refers to the use of a web browser for learning. It has been widely used both as a learning tool to support formal programs and as a means of delivering online learning programs. In the literature, two main issues are addressed in web-based learning environments, namely the design of the learning materials and the technology. In the last decade, teachers have gained experience in the design of learning materials (online activities, games, animations, and simulations) with easy-to-use software tools. These materials also improved learning and made it more enjoyable for learners (Tavangarian et al., 2004). With advanced information and communication technologies, many technological barriers, such as limited and poor communication access and slow downloading of images and videos, are eliminated in web-based learning environments.

However, learner needs and experience must still be considered. Appropriate technology and reasonable computer skills are needed to get the best out of web-based learning, which, during the COVID-19 pandemic, led to the use of various online platforms for different courses. Figure 1 shows some of the various online systems, for example Clever, used by a number of schools in which students would have access to landing pages of various online platforms that they would use for schoolwork, such as Google Classroom, Canvas, Google Drive, Office 365, etc. They also had links to online textbooks, applications, and popular apps used in the instruction.

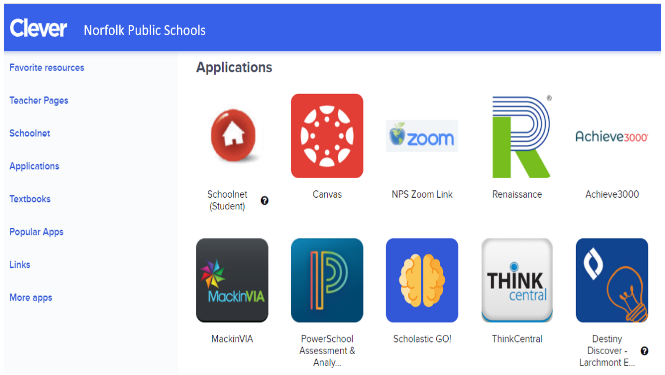


Figure 1. Clever landing page of Norfolk Public Schools.

Online learning is usually described as access to learning experiences via the use of some technology or as a more recent version of distance learning, which improves access to educational opportunities for learners (Moore, Dickson-Deane & Galyen, 2011). This form of virtual learning became more popular with internet technologies and is associated with electronic content available on a computer/mobile device. Online learning can be conducted through programs or apps installed on a user's devices. It provides many advantages, such as increasing student engagement, making it easier to differentiate instruction, which saves time with planning and grading. However, online learning relies on students having access to technology in school on a regular basis. Online learning works best for middle and high school teachers who want to provide different ways for their students to learn (Moore et al., 2011).

Distance learning is described as the effort of providing access to learning for those who are geographically distant. Distance learning is an excellent teaching method, because they need the flexibility to contend with competing priorities (Galusha, 1998). It does not have to be conducted with electronic and web-based technologies. It can be conducted through the use of audio-video media, such as videotape or DVDs (Holden & Westfall, 2007). Distance learning provides greater flexibility for students to work at their own pace and review work as needed. With the development of digital technologies, distance learning is increasingly associated with online learning. Distance learning is a method for delivering instruction solely online and does not include any in-person interaction between teachers and students. It is not feasible to use distance learning if the students do not have access to devices or the internet at home. Distance learning typically works best with older students who have consistent technology access at home and will work responsibly on their own (Stauffer, 2020).

Blended learning is a type of learning that combines virtual and traditional forms of teaching (Kim, 2007). It covers online resources and allows control of the learning process in terms of time, place, and learning method. Blended learning is also used to describe learning that mixes various event-based activities, including face-to-face classrooms, live e-learning, and self-paced learning (Valiathan, 2002). Blended learning can also be viewed as a kind of relic, symbolic of the gap between traditional education and connected and digital learning. It includes face-to-face group work in a classroom, then going home to analyze that work and turning in an assessment individually or taking a course online, then receiving face-to-face tutoring between online lessons (TeachThought, 2020). Blended learning provides many advantages in terms of flexibility, effectiveness, teacher empowerment, engagement, and differentiation. However, it requires training and support in technology usage for teachers, advanced information and communication technologies, and tools to provide the required environment of a blended learning classroom (Walker, 2018).

Virtual learning is a type of educational technology environment that is typically offered as a web-based learning platform utilizing computers and internet technologies. It is associated with things like online courses, tools, simulations, e-textbooks, and e-workbooks. It consists of many educational components, activities, and interactions, such as content, curriculum mapping and planning, learner engagement and administration, communication and collaboration, and real-time communication—live video conferencing or audio conferencing (Stiles, 2000). For virtual learning, all teaching activities are carried out in an online environment—either self-paced (asynchronous) or live web-conferencing (synchronous)—in which the teacher and students are physically separated (Skylar, 2009). It provides many advantages over traditional forms of education, such as remote access, an individualized learning process, a safe and secure learning environment, flexible learning in terms of time, location, and place, cost-effectiveness, time-efficiency, and scalability. Many of these learning modes have been used by various institutions, either in high schools, colleges, or universities. Some distance learning occurred with paper-based packets in the Norfolk Public Schools at the end of the 2019-20 academic year, when the COVID-19 pandemic caused schools to close and while many students still did not have access to the internet or have reliable devices to assist them in the real-time distance learning.

Some of the modules developed during this project were designed for "Learning in Place" paper-based packets that were distributed to high school students. They were supposed to be stand-alone, paper-based modules that could be completed independently by students. One of the main issues was related to the nature of the computer science and cybersecurity disciplines themselves, as they are heavily related to the use of computers and some informational technology (IT). However, back when they were in school, several members of the research team did learn the basics of programming and computer science without the use of computers, and they went back to the drawing board and rethought the approach of teaching intro to computer science and cybersecurity courses. The main idea was to take the students back to the basics, back to the motivation behind the cryptography and cyphers, back to the basics related to programming and the way networking was structured and start from there. There was a need to investigate what kinds of things should be taught at each step of the computer science and cybersecurity pathway and how this high school knowledge was connected to the profession of engineering and engineering technology.

The main idea was to teach these topics through application-based activities and hands-on approaches and to expose the students to industry and academics through a series of visiting speakers whom they would otherwise not meet. All five Norfolk Public Schools high schools have students from qualified opportunity zones that have populations from low-socioeconomic levels (Jovanovic et al., 2020), and many students did not have adequate devices and internet access when the pandemic started.

Policy Issues in Teaching Computer Science and Cybersecurity

Attention to cybersecurity education has been growing at the federal level since January 2008, when President George W. Bush launched the Comprehensive National Cybersecurity Initiative (CNCI). The following year, President Barack Obama conducted a review of security issues and efforts and implemented 12 strategies in support of the CNCI (The White House of President Obama, 2011). In February of 2014, then Governor of the Commonwealth of Virginia Terry McAuliffe established Cyber Virginia and the Virginia Cyber Security Commission through Executive Order 8.

Presenting recommendations to foster an improved cybersecurity workforce pipeline was among the responsibilities of the commission. It was determined that there was an immediate need to identify the role of K-12 education in building the cybersecurity pipeline, as well as to help schools at all levels—elementary, middle, and high school—prepare students for the cybersecurity career field. Since cybersecurity affects all occupations, CTE pathway courses were customized for each of the 16 career clusters. Virginia developed a cybersecurity pathway to be implemented in middle and high schools (Virginia Department of Education, 2016). In the fall of 2017, high school students could enroll in one of four new pathways: Programming and Software Development, Health and Medicine Sciences, STEM/ Pre-Engineering Technology, and Network Systems.

Standards and Interoperability

The CTE Federal Program Monitoring Review System (Virginia Department of Education, 2020a) was designed to focus on continuous program improvement and student achievement. The Federal Program Monitoring Review System consists of three phases: Phase I requires the school division to conduct a comprehensive CTE self-assessment on a six-year cyclical schedule and develop a program improvement plan, as needed, to address identified deficiencies and concerns; Phase II requires the VDOE to conduct an analysis of the self-assessment report and other relevant data that may include an on-site visit to review specific CTE programs; Phase III requires the school division to follow up on any identified deficiencies and concerns.

Superintendent Memo #162-19, Virginia Department of Education, dated July 10, 2020, states that the 2020 General Assembly is continuing state funding to support industry credentialing testing materials for students and professional development for instructors in science, technology, engineering, and mathematics-health sciences (STEM-H) CTE programs. This appropriation is from the lottery proceeds fund and included $500,000 for fiscal year 2021.

Tools and Systems in e-Learning of Computer Science and Cybersecurity

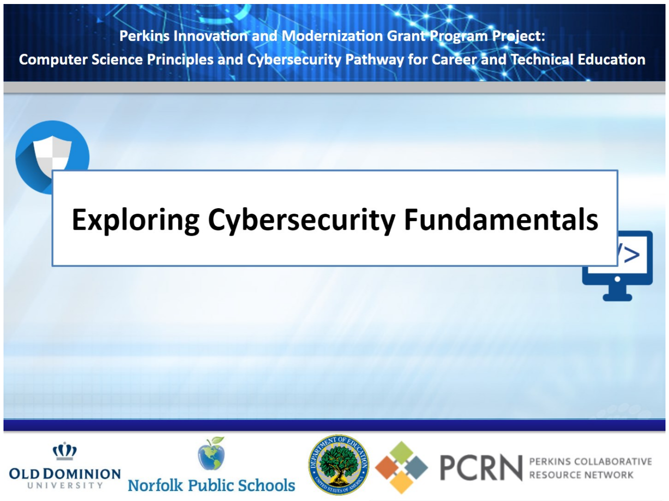
Norfolk Public Schools decided to focus on a distance learning approach of virtual learning that included the teacher, not just the facilitator. Various virtual learning tools were used: simulations, e-textbooks, e-workbooks, Virginia Cyber Range—a scalable, cloud-hosted infrastructure providing students with virtual environments for realistic, hands-on cybersecurity labs and exercises (Raymond, 2020), and resources available on other platforms, such as on cyber.org and code.org. In virtual learning, teachers are teaching synchronously, and they are not using asynchronously pre-recorded lectures. Students do have meetings with their teachers. They are also using MindTap accounts (Cengage, 2020).

At the end of the 2019-2020 school year, paper packets, called Learning-in-Place packets, included all necessary materials that students were using and Google Classroom and Google Drive materials and testing. The issue was that not all K-12 students in the Norfolk Public Schools had access to the internet and devices that they could use to participate in virtual learning. Because of this, initial learning happened through the paper-based approach. In the case of computer science and cybersecurity, the main problem was related to teaching something so dependent on information technology without information technology. The Norfolk Public School system has utilized the Google Suite of tools; however, they are currently moving to the Canvas educational learning management system. Other school districts in the area, such as Virginia Beach Public Schools and Chesapeake Public Schools, were already using Schoology (Schoology, 2020) and students already had mobile devices such as Chromebooks provided by the school system (Google, 2020).

Content Development

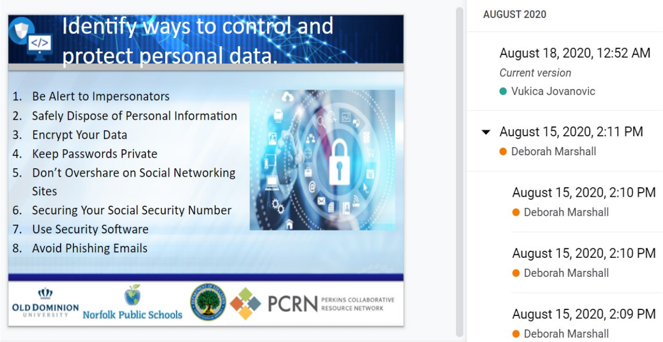
In the fall of 2017, the Norfolk Public Schools were given permission by the Virginia Department of Education to offer cybersecurity fundamentals at all five of its high schools. The research team focused on the development of educational modules for two CTE courses under the Business and Informational Technology career cluster: Cybersecurity Fundamentals and Informational Technology (IT) Fundamental course (Virginia Department of Education, 2020b). These two courses were identified to be in the most demand and were implemented in all five Norfolk Public Schools. Both courses have a duration of 36 weeks and include the same set of competencies (1-38). These are: Workplace Readiness Skills for the Commonwealth of Virginia, Examining All Aspects of an Industry, Addressing Elements of Student Life, and Exploring Work-Based Learning. Competency 39 begins with the specific course competencies.

From June to August of 2020, Old Dominion University undergraduate and graduate students created Google Slides with educational modules based on the Virginia Department of Education's Career and Technical Education course competencies. The principal investigator created the template for all modules. They all had a unified design and information about the main stakeholders in each one of the slides. Each slide had one task/competence at the beginning. Some of them were expanded on multiple slides. Visuals were retrieved from Google Images with filtering of images approved for public reuse. Figure 2 shows an example of one such module. As the graduate and undergraduate students progressed with the development of the Google Slides modules, Norfolk Public Schools Career & Technical Education faculty, Dr. Deborah Marshall and Mr. Michael Crespo, provided feedback on each of the Google Slides, which was disseminated to all of the team members for further comments. Figure 3 shows one example of version control.


Perkins Innovation and Modernization Grant Program Project:
Computer Science Principles and Cybersecurity Pathway for Career and Technical Education

Exploring Cybersecurity Fundamentals

Figure 2. Example of one educational module in Google Slides.


Identify ways to control and protect personal data.

1. Be Alert to Impersonators
2. Safely Dispose of Personal Information
3. Encrypt Your Data
4. Keep Passwords Private
5. Don't Overshare on Social Networking Sites
6. Securing Your Social Security Number
7. Use Security Software
8. Avoid Phishing Emails

AUGUST 2020

August 18, 2020, 12:52 AM
Current version
Vukica Jovanovic

August 15, 2020, 2:11 PM
Deborah Marshall

August 15, 2020, 2:10 PM
Deborah Marshall

August 15, 2020, 2:10 PM
Deborah Marshall

August 15, 2020, 2:09 PM
Deborah Marshall

Figure 3. Digital thread management was done with the version control in Google Docs.

Additional videos were created with hands-on activities and voiceovers. These modules were created to assist teachers with virtual, hybrid, or face-to-face versions of the Cybersecurity Fundamentals and Information Technology (IT) Fundamentals courses.

Data Collection and Analysis

The industrial advisory board had representatives that were IT and cybersecurity professionals from the following industries: government employees, shipbuilding, rotating machinery manufacturers, banking, consumer products industry, robotics industry, automotive industry, cybersecurity initiatives, and community college cybersecurity pathway experts. Additional professionals were recruited through the use of the social platform LinkedIn. The research team also worked with a professional instructional developer to finalize the modules and to implement suggestions from industry practitioners. The finalized modules were distributed to the CTE cybersecurity teachers in the Commonwealth of Virginia in April of 2021 through Judith Sams, Teacher Specialist for Business and Informational

Technology pathways, who works in the Virginia Department of Education. They were distributed through the project website https://sites.wp.odu.edu/odu-nps-cs-cybersecurity-pathway-for-cte/ (Jovanovic, 2019). IT Fundamentals modules were reviewed by 33 industry participants and the cybersecurity modules were reviewed by five industry participants. Figure 4 shows one such review example.

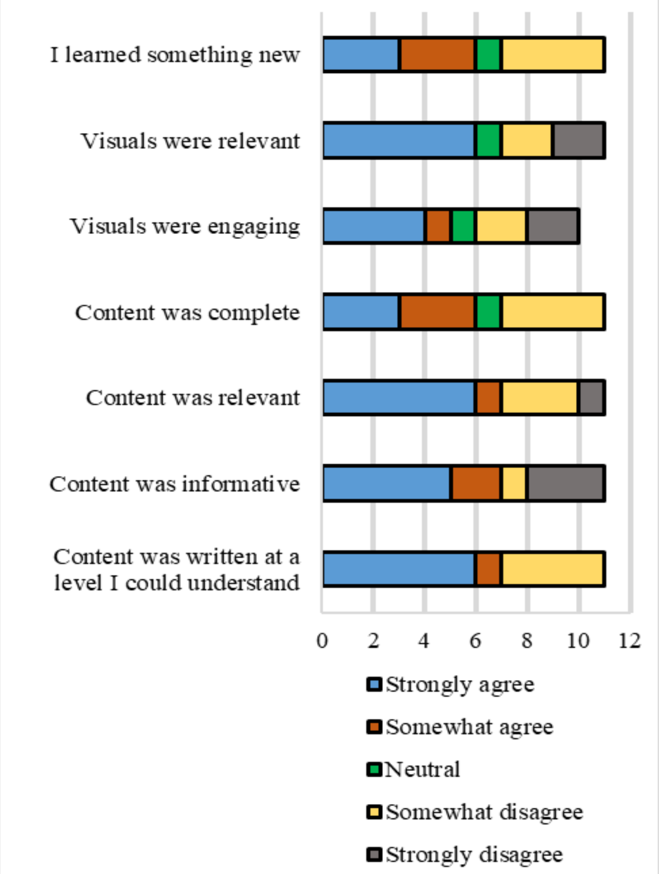


Figure 4. One example of quantitative industry feedback for an educational module from the course IT Fundamentals ITF Tasks 39-57: Mastering Digital Technology Basics

Finalized modules were disseminated across Virginia. Data were collected from six other school districts: Martinsville City Public Schools, Montgomery School Division, York County School Division, Charlotte County Public Schools, Roanoke County Public Schools, and Henry County Public Schools for IT Fundamentals. Sixty percent of respondents were actively teaching information technology fundamentals, 40% were not. They like to teach that course, because they like learning and teaching about computers, they feel that students can benefit from this course, that it is very relevant, and that it has a variety of content areas. The biggest challenges that the teachers saw when teaching IT fundamentals were that it had limited hands-on projects, programming issues, and, since it was an elective course, students would not always sign up.

They also reported challenges finding materials for their lessons. When asked to identify the cause of problems teaching an IT fundamentals course, they said that technology changes very fast, budgets were limited, and that they had very little knowledge on how to program. They agreed that up-to-date course materials, hands-on equipment would help them teach this course. They also noted that they would need equipment for simulations and network access. They further noticed that they were spending a great deal of time developing lesson plans. All of the teachers who participated in this study noted that the content was written at a level that they could understand and that the content was informative. Sixty percent somewhat agreed and 30% strongly agreed that the content was relevant, visuals were engaging and relevant, and that they learned something new. The only neutral comment was that the "content was complete." There were no comments in the "somewhat disagree" and "strongly disagree" categories. Some of the teachers noted that it was hard for them to answer some questions until they had a chance to teach the material, since this course was new for most of them.

The following school districts responded to a survey related to the Cybersecurity Fundamentals modules: Chesterfield County, Roanoke City Public Schools, Rockbridge County Schools, Fredericksburg City Schools, Loudoun County Public Schools, Essex County Public Schools, Charlotte County Public Schools, Cumberland County, Wythe County Public Schools, Newport News Public School, Norfolk Public Schools, Fairfax County Public Schools, and York County Public Schools. Seventy-three percent of the teachers who responded to this survey were already teaching a Cybersecurity Fundamentals course at their school in Virginia. Only one teacher outside of Virginia reported teaching this course, while five others said that they were not yet teaching the course. They noted that they like teaching this course, because it helped them build experience with computer technology and that students could use their knowledge about internet safety even if they did not choose to go into the cybersecurity field. Another teacher noted that the course was a broad mix of topics with many different aspects—it had elements of history, computing, politics, psychology, etc.

Other teachers reported that they did not enjoying teaching this course, since they had not received any training and that there was no available curriculum. They also mentioned difficulties related to transferring all courses to the virtual mode, due to the COVID-19 pandemic. Other teachers noted that it was a current topic and that it should be emphasized in the school system, since there were great opportunities in this field. Some noted that they loved the opportunity to prepare their Title 1 students for the careers out of high school, since the students could obtain certifications that could enable them to work as helpdesk technicians. Some others noted that the class was interesting and challenging. They noted that students loved the classes and enjoyed learning about different threats and that they better understand the need for cyber professionals. The class topics assisted students in gaining tools needed to appreciate and understand existing cybersecurity threats and to learn how to mitigate them. It was also reported that the students enjoyed learning about the implications of cybersecurity in their daily lives and liked the hands-on activities related to the course. Finally, one teacher noted that they liked the relevance of the content and hoped to inspire students to pursue cybersecurity as a career.

Teachers noted that the biggest challenges or barriers when teaching a cybersecurity fundamentals course were: learning how to do things that they have never done before; keeping student interest going forward throughout the school year; the subject required a lot of critical thinking; and, most Freshmen want to be led through things rather than figuring them out for themselves. Other problems were related to the lack of teacher training and clarity of expectations. They noted that it was difficult to ascertain the level of depth to which they should be addressing the materials from a list of objectives. They noted that it would have been nice to have teacher resource materials and that teachers needed more than just a scenario, they needed answers, outcomes, and expectations. Others agreed that they did not have access to existing curricula for cybersecurity and that they needed more knowledge and more training to gain confidence in the topics.

Teachers also identified challenges in finding and using exercises in a virtual simulated environment, where students could really practice the command-line interfaces and methods used in navigating, configuring, and securing network systems. Teachers suggested that it would be good to develop a logical scope and sequence for the course that uses a building-block, scaffolding approach. They also emphasized that finding and/or creating practical, engaging, real-world labs, activities, and assignments would help them to develop a better teaching and learning environment. They noted that it was hard to browse through the large volume of resources that were available for finding materials that aligned with their vision of what should be taught and how it should be taught within the constraints of the course competencies.

Teachers agreed that the main cause of problems while teaching this course was a lack of available resources. Another problem was that this was a hard subject that required more work than students were accustomed to doing in an elective class. Moreover, they did not have enough financial support from the school system and they themselves did not have such courses while in college. They noted that they needed technology, firewalls, and protocols in place for this class. They also identified the problem that a lot of the cybersecurity resources were very text heavy and did not include any hands-on activities. Others noted that their local computers were locked down so that students could not access operational system configuration or networking features.

When asked to propose a solution that could help them to teach a cybersecurity fundamentals course, teachers suggested that training was the most important thing along with a complete set of curriculum materials. They suggested that the students should be incentivized to get a certification. They noted that even though they did receive invites for some workshops and training, it was hard to find time to attend all required professional development workshops. Some noted that students needed real computers not Chromebooks. They think that they should also apply for grants and donations and keeping machines off the network. The suggested that cyber careers should be mentioned in lower grades and the cyber jobs should be promoted. Teachers agreed that having these slides available in the central repository was a good start to make teaching this class easier. They noted that teachers should collaborate in the development of a curriculum that could be shared.

All teachers agreed that the content was written at a level that they could understand and that the content was relevant and informative. They agreed that visuals were relevant and that they learned something new. Some teachers noted that the content was not complete, as the topic was very broad. Some noted that it was a good place to start but that it should be improved and include the required depth that could give students an adequate understanding of concepts.

Hands-on Modules

One of the main challenges with distance learning is getting students engaged and perform hands-on activities that increase their understanding of cybersecurity and related applications. Another significant challenge is the need for hardware, such as computers, networking devices, electronics components, materials, as well as an internet connection needed for some hands-on activities. Moreover, it is always hard to run hands-on cybersecurity activities, due to their complexity and the relative high cost of hardware. Distance learning, and the lack of interaction with instructors and peers, makes it even more difficult. For all of these reasons, the approach considered for the practical side of this current project was to first conduct simple, hand -solved activities and then follow them up with hardware-based, more complex activities, developed to help students understand real-world cybersecurity applications.

The research team developed both types of hands-on activities to be conducted with high school students: Introduction to Cryptography and Ciphers was a first step towards cybersecurity with pencil-and-paper type activities; Internet-of-Things (IoT) with Arduino was a hardware-based activity. Students enjoyed both types of activities, but they found the hardware-based ones more difficult, due to their own lack of background and experience with hardware and the IoT concept. The limited time to deliver the activities made it harder for students to grasp concepts from scratch and be able to work on applications other than at the basic level. It is also important to note that, while most students were using tablets, smartphones, other electronic devices, and in smaller amounts personal computers, they were very intimidated by learning programming and writing their own code. It was for such cyber-related activities to develop student interest in programming and help them make the transition from simple users of software products to actual developers of them.

Dissemination

The presentations were released to Cybersecurity Fundamentals and IT Fundamentals teachers for classroom use and evaluation to Norfolk Public Schools CTE teachers on August 26, 2020. The need for any supplemental teaching materials was so high that the modules were distributed to teachers even before they were finalized. They were distributed to three high schools that offered these two classes and they will be distributed to all five high schools in the Norfolk Public School system in the 2021-22 academic school year. They were reviewed by the CTE teachers and industry cybersecurity practitioners in the fall of 2020. The research team also met with industry representatives and invited them to form an industrial advisory board for the project and to provide feedback for module improvements. Teachers had a professional development workshop in August of 2020. Ninety percent of the teachers strongly agreed that availability of these modules was empowering teachers to teach cyber courses. One teacher noted that they could use the knowledge and skills gained during this professional development activity to impact student learning.

Conclusions

One of the main challenges with distance learning is to engage students in active hands-on activities that increase their understanding of cybersecurity and related applications. The other challenge is the need for hardware, such as computers, networking devices, electronics components, materials, etc., in some hands-on activities. It is required to build a virtual learning system with online education and tools, to be able to create a more resilient and educated society for the next generations. Otherwise, the current crisis may cause a worldwide, large-scale issue. Virtual learning environments have been widely used to access information and communication technologies and broadband internet technologies for many years in higher education. It is also becoming more common in high schools, due to COVID-19 and related regulations in recent years. It is expected that virtual learning will be used significantly in all levels of education in the future. However, in order for this to work, resources are needed, such as broadband internet technologies, computers, and environments that support virtual learning through online education and tools. Students should have access to those resources in order to be able to continue virtual learning through the internet or television. In addition, teachers should adapt to new pedagogical concepts and educational modules to teach remotely.

In this paper, the authors presented one initiative to help CTE teachers to quickly adapt to the needs of the new online courses, which is not yet reflected as part of the undergraduate training in the programs that prepare future CTE teachers in this emerging area of cybersecurity. By this method, university faculty can assist high school teachers in teaching the relevant content verified by the incumbent workforce. Students can also be exposed to engineering and engineering technology careers, and, in the long run, educators can create and sustain stronger educational pathways to STEM degrees.

Acknowledgement

The project team wishes to acknowledge funding received by the U.S. Department of Education, Office of Career, Technical, and Adult Education, Division of Academic and Technical Education, Innovation and Modernization Program, award # V051F190072, grant #12882683, funded by the Perkins V statute, U.S. Congress.

References

Aliyyah, R. R., Rachmadtullah, R., Samsudin, A., Syaodih, E., Nurtanto, M., & Tambunan, A. R. S. (2020). The Perceptions of Primary School Teachers of Online Learning during the COVID-19 Pandemic Period: A Case Study in Indonesia. *Journal of Ethnic and Cultural Studies*, *7*(2), 90-109.

Cengage. (2020). *Mindtap*. Retrieved from https://www.cengage.com/mindtap/

Galusha, J. M. (1998). *Barriers to learning in distance education*. University of Southern Mississippi. Retrieved from https://files.eric.ed.gov/fulltext/ED416377.pdf

Google. (2020). *Google Chromebooks*. Retrieved from https://www.google.com/chromebook/

Hoffman, J. A., & Miller, E. A. (2020). Addressing the Consequences of School Closure Due to COVID-19 on Children's Physical and Mental Well-Being. *World Medical & Health Policy, 12*(3), 300-310.

Holden, J. T., & Westfall, P. J. L. (2007). *An Instructional Media Selection Guide for Distance Learning*. Fourth Edition. United States Distance Learning Association. Retrieved from https://files.eric.ed.gov/fulltext/ED501248.pdf

Horton, W. (2011). *e-Learning by Design*: John Wiley & Sons.

Jovanovic, V. M., Kuzlu, M., Popescu, O., Badawi, A. R., Marshall, D. K., Sarp, S. …Wu, H. M. (2020, June). *An Initial Look into the Computer Science and Cybersecurity Pathways Project for Career and Technical Education Curricula*. Paper presented at The American Society for Engineering Education 2020 ASEE Virtual Annual Conference, Computing and Information Technology Division. Virtual Online. June 22-26, 2020. Retrieved from http://dx.doi.org/10.18260/1-2--3412

Kim, W. (2007). *Towards a Definition and Methodology for Blended Learning*. Paper presented at the Workshop on Blended Learning 2007, August 2007. Edinburgh, United Kingdom. 1-8. Pearson.

Moore, J. L., Dickson-Deane, C., & Galyen, K. (2011). e-Learning, online learning, and distance learning environments: Are they the same? *The Internet and Higher Education*, *14*(2), 129-135.

The White House of President Obama (2011). *The Comprehensive National Cybersecurity Initiative*. Foreign Policy. Retrieved from https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

Jovanovic, V. (2019). *Computer Science and Cybersecurity Pathway for Career and Technical Education project website*, Old Dominion University, Retrieved from https://sites.wp.odu.edu/odu-nps-cs-cybersecurity-pathway-for-cte/

Radha, R., Mahalakshmi, K., Sathis Kumar, V., & Saravanakumar, A. (2020). E-learning During Lockdown of Covid-19 Pandemic: A Global Perspective. *International Journal of Control and Automation*, *13* (4), 1088-1099.

Raymond, D. (2020). *Virginia Cyber Range*. Retrieved from https://www.virginiacyberrange.org/

Schoology. (2020). *Schoology: Learning Management System*. LMS. Retrieved from https://www.schoology.com/

Skylar, A. A. (2009). A Comparison of Asynchronous Online Text-Based Lectures and Synchronous Interactive Web Conferencing Lectures. *Issues in Teacher Education*, *18*(2), 69-84.

Stauffer, B. (2020). *What's the Difference between Online Learning and Distance Learning?* Applied Educational Systems. Retrieved from https://www.aeseducation.com/blog/online-learning-vs-distance-learning

Stiles, M. (2000). Effective Learning and the Virtual Learning Environment. Paper presented at the *EUNIS 2000 – Towards Virtual Universities*, Instytut Informatyki Politechniki Poznanskiej. Poznan University of Technology. Poznan, Poland. April. 2000, ISBN 83 913639.

Tavangarian, D., Leypold, M. E., Nölting, K., Röser, M., & Voigt, D. (2004). Is e-Learning the Solution for Individual Learning? *Electronic Journal of E-learning*, *2* (2), 273-280.

TeachThought. (2020). *The Definition of Blended Learning*. Retrieved from https://www.teachthought.com/learning/the-definition-of-blended-learning/

Valiathan, P. (2002). Blended Learning Models. *Learning Circuits*, *3*(8), 50-59.

Virginia Department of Education. (2016). *Virginia's 21st Century Pathway: Cybersecurity*. Virginia Department of Education, Richmond, Virginia. Retrieved from http://doe.virginia.gov/instruction/career_technical/cybersecurity/cybersecurity-white-paper.pdf

Virginia Department of Education. (2020a). *Program Administration and Management*, Virginia Department of Education, Richmond, Virginia. Retrieved from http://www.doe.virginia.gov/instruction/career_technical/administration/

Virginia Department of Education. (2020b). *Business and Information Technology Virginia CTE Resource Center (VERSO)*. Virginia Department of Education, Richmond, Virginia. Retrieved from http://www.cteresource.org/curriculum/business-and-information-technology/index.html

Virginia Department of Education. (2019a). *Information Technology Fundamentals*. Virginia Department of Education, Richmond, Virginia. Retrieved from http://www.cteresource.org/curriculum/business-and-information-technology/Information%20Technology%20Fundamentals%206670.pdf

Virginia Department of Education. (2019b). *Cybersecurity Fundamentals*. Virginia Department of Education, Richmond, Virginia. Retrieved from http://www.cteresource.org/curriculum/business-and-information-technology/Cybersecurity%20Fundamentals%206302.pdf

Walker, S. (2018). 5 Benefits of Blended Learning. *Imagine Learning*. Retrieved from https://www.imaginelearning.com/blog/2018/09/5-benefits-blended-learning

Appendix

Task competencies for course # 6670: Information Technology (IT) Fundamentals. These tasks were developed by the Virginia Department of Education's CTE Resource Center (Virginia Department of Education, 2019a). They are provided here just to explain which modules were developed.

Mastering Digital Technology Basics

39. Investigate the history and emerging advances of digital technology
40. Describe the effect of digital technology on business and society.
41. Describe software associated with information systems.
42. Explore binary concepts and their operations in the digital technology world.
43. Describe the evolution of the Internet and how it works.
44. Investigate emerging technologies as they relate to the future of the Internet.
45. Investigate trends in digital technology.
46. Examine social, ethical, and legal issues associated with digital technology.
47. Debate an ethical issue related to using computer and Internet technology.

Using Digital Applications

48. Create documents related to real-world business situations.
49. Create a relational database for a real-world business situation.

50. Create spreadsheets for a real-world business situation.
51. Create presentations related to a real-world business situation.

Investigating Computer Fundamentals

52. Identify the parts of a computer system and the relationships among its components.
53. Describe characteristics and functions of CPUs.
54. Explain the functions and characteristics of system expansion devices.
55. Demonstrate the use of connectivity devices and peripheral equipment.
56. Perform basic operations in an operating system environment.
57. Manage various file types.
58. Describe the computer start-up sequence.
59. Compare operating systems.
60. Investigate needs affecting system purchases and upgrade decisions.
61. Investigate the building stages of a computer.

Maintaining, Upgrading, and Troubleshooting Computers

62. Describe the importance of system maintenance and preventive measures.
63. Install hardware in a computer system.
64. Install software programs.
65. Explain the purpose of anti-X software.
66. Identify problems associated with computer hardware, operating systems, and application software.
67. Describe risk-mitigation techniques.
68. Identify security risks inherent to computer hardware and software.
69. Describe security best practices for businesses.
70. Describe the importance of data backup media and strategies.
71. Back up files.
72. Evaluate remote connection troubleshooting.

Exploring Network Fundamentals

73. Investigate networks and their evolution.
74. Explain networking concepts and different network structures.
75. Compare peer-to-peer and client-server networks.
76. Describe the differences between analog and digital technologies.

Exploring Internet Fundamentals

77. Identify the necessary elements that are required to connect to the Internet.
78. Describe the concept of IP addresses and the Domain Name System (DNS).
79. Explain the delivery methods of ISPs.
80. Compare the types and features of various web browsers.
81. Explain file transfer mechanisms.
82. Exhibit principles of digital citizenship.
83. Identify criteria for conducting searches on the Internet.
84. Assess the effect and value of available firewalls and intrusion detection systems (IDS).

Exploring Programming

85. Explain the purpose and functions of computer programming.
86. Identify the types of programming languages.
87. Explain the steps in a program life cycle.
88. Design a simple program for a specific application.
89. Create a simple computer program.
90. Execute a simple program.
91. Document a simple program.

Exploring Web Page Design

92. Investigate design elements of professionally developed websites.
93. Analyze the navigation of a website for ease of use.
94. Create a website.
95. Investigate publishing a website.

Exploring Graphics and Interactive Media

96. Identify hardware required for multimedia and entertainment presentations.
97. Identify software programs associated with graphics and interactive media.
98. Explore the components of multimedia design and their applications.
99. Explore digital technology as it relates to game design and development.
100. Create an interactive multimedia presentation.

Preparing for Industry Certification

101. Describe the process and requirements for obtaining industry certifications related to the IT Fundamentals course.
102. Identify testing skills/strategies for a certification examination.
103. Demonstrate ability to successfully complete selected practice examinations.
104. Complete an industry certification examination representative of skills learned in this course.
105. Complete self-assessments to help determine career development goals.
106. Investigate careers, educational requirements, and certifications in the IT career pathways.
107. Demonstrate project-management skills.
108. Create manual and online employment-related correspondence.
109. Create an electronic and/or hard-copy portfolio.

Task competencies for course # 6302: Cybersecurity Fundamentals. These tasks were developed by the Virginia Department of Education' CTE Resource Center (Virginia Department of Education, 2019b).

Exploring Computer Concepts

39. Describe cybersecurity.
40. Define information assurance.
41. Describe the critical factors of information security.
42. Explain cybersecurity services as they relate to intrusion prevention capabilities that protect systems against unauthorized access, exploitation, and data exfiltration.
43. Define risk.
44. Identify the concepts of cybersecurity risk management.
45. Describe cybersecurity threats to an organization.
46. Explain why organizations need to manage risk.
47. Discuss national or industry standards/regulations that relate to cybersecurity.
48. Describe the cyber-attack surface of various organizations.
49. Analyze risks affecting critical infrastructure.

Examining Computer Networks as a Foundational Element of Cybersecurity

50. Describe a network.
51. Describe a wired/cabled network.
52. Describe a wireless network.
53. Compare cabled/wired and wireless networks.
54. Compare networking conceptual models.
55. Discuss services, their relationship to the OSI model, and potential vulnerabilities.
56. Differentiate among network types.
57. Examine the concept of the Internet as a network of connected systems.
58. Identify networking protocols.

Understanding Cyber Threats and Vulnerabilities

59. Describe the difference between a cyber threat and a vulnerability.
60. Describe types of cyber threats.
61. Analyze types of current cyber threats.
62. Identify the perpetrators of different types of malicious hacking.
63. Describe the characteristics of vulnerabilities.
64. Identify the prevention of and protections against cyber threats.
65. Identify the cyber risks associated with bring your own device (BYOD) opportunities on computer networks.

Exploring Ethics as it Relates to Cybersecurity

66. Differentiate between ethics and laws.
67. Distinguish among types of ethical concerns.
68. Define cyberbullying.
69. Identify actions that constitute cyberbullying.
70. Identify possible warning signs of someone being cyber bullied.
71. Identify laws applicable to cybersecurity.
72. Explain the concept of "personally identifiable information."
73. Explain how and why personal data is valuable to both an individual and to the organizations (e.g., governments, businesses) that collect it, analyze it, and make decisions based on it.
74. Identify ways to control and protect personal data.
75. Demonstrate net etiquette (netiquette) as it relates to cybersecurity.
76. Analyze the social and legal significance of the ongoing collection of personal digital information.

Examining Data Security as it Relates to Cybersecurity

77. Distinguish between data, information, and knowledge.
78. Identify the most common ways data is collected.
79. Identify the most common ways data can be stored.
80. Explain the difference between data at rest, data in transit, and data being processed.
81. Identify the most common ways data is used.
82. Discuss how data can be compromised, corrupted, or lost.
83. Explain how businesses and individuals can protect themselves against threats to their data (e.g., firewalls, encryption, disabling, backups, and permissions).

Securing Operating Systems

84. Define the function of a computer operating system.
85. Identify the components of an operating system.
86. List types of operating systems.
87. Evaluate the potential vulnerabilities, threats, and common exploits to an operating system.
88. Identify best practices for protecting operating systems.
89. Describe the concept of malware and techniques to guard against it.
90. Evaluate critical operating system security parameters.
91. Describe security and auditing logs.
92. Describe the role of a system backup.
93. Define virtualization technology.
94. Identify advantages and disadvantages of using virtual machines.

Programming as a Component of Cybersecurity

95. Define programming in the context of cybersecurity.
96. Differentiate between computer programming languages.
97. Evaluate common programming flaws that lead to vulnerabilities.
98. Identify best practices in secure coding and design.

Exploring Cybersecurity Implications for Current and Emerging Technologies

99. Identify ubiquitous computing.
100. Discuss security and privacy implications of ubiquitous computing.

Exploring Cybersecurity Careers

101. Research career opportunities for cybersecurity professionals.

102. Explore the Career Clusters affected by current and emerging technology.
103. Identify the educational pathways for emerging cybersecurity professionals.
104. Identify career paths and job titles within the cybersecurity/cyber forensics industry and Career Clusters.
105. Research the cyber threats and security measures related to career pathways.

Preparing for Industry Certification

106. Identify testing skills/strategies for a certification examination.
107. Describe the process and requirements for obtaining industry certifications related to the Cybersecurity Fundamentals course.
108. Demonstrate the ability to complete selected practice examinations (e.g., practice questions similar to those on certification exams).
109. Successfully complete an industry certification examination representative of skills learned in this course (e.g., Microsoft, IC3, and CompTIA).

Biographies

VUKICA JOVANOVIC is the Interim Chair, Batten Fellow, and Associate Professor of Engineering Technology at Old Dominion University She holds a PhD from Purdue University, Magistar (PhD candidate) degree in industrial engineering and management, focused and dipl. ing. degrees from the University of Novi Sad, Serbia. She has funded research in broadening participation efforts of underrepresented students in STEM funded by the U.S. Department of Education, focusing on computer science and cybersecurity pathways, and from the Office of Naval Research, focusing on mechatronic pathways. She is part of the ONR projects related to the additive manufacturing training of the active military. She is also part of the research team that has multiple projects funded by the NSF, focusing on veteran pathways and their success in engineering. She leads the team that delivers the summer program to ninth graders that focuses on broadening the participation of underrepresented students into STEM (ODU BLAST), funded by the Virginia Space Grant Consortium. Dr. Jovanovic may be reached at v2jovano@odu.edu

MURAT KUZLU is an assistant professor of engineering technology at Old Dominion University. He received his BSc, MSc, and PhD degrees in electronics and telecommunications engineering from Kocaeli University, Turkey, in 2001, 2004, and 2010, respectively. From 2005 to 2006, he worked as a Global Network Product Support Engineer at Nortel Networks, Turkey. In 2006, he joined the Energy Institute of TUBITAK-MAM (Scientific and Technological Research Council of Turkey – The Marmara Research Center), where he worked as a senior researcher. Before joining ODU, he worked as a research assistant professor at Virginia Tech's Advanced Research Institute. His research interests include smart grid, demand response, smart metering systems (AMR, AMI, and AMM), home and building energy management systems, co-simulation, wireless communications, and embedded systems. Dr. Kuzlu may be reached at mkuzlu@odu.edu

OTILIA POPESCU is an associate professor of engineering technology and the program director of the electrical engineering technology program at Old Dominion University. She received her Engineering Diploma and MS degree from the Polytechnic Institute of Bucharest, Romania, and PhD degree from Rutgers University, all in electrical and computer engineering. Her research interests include the general areas of communication systems, control theory, signal processing, and engineering education. In the past, she has worked for the University of Texas at Dallas, the University of Texas at San Antonio, Rutgers University, and the Politehnica University of Bucharest. Dr. Popescu may be reached at opopescu@odu.edu

PETROS KATSIOLOUDIS is a full professor and Chair of STEM and Professional Studies at Darden College of Education and Professional Studies at Old Dominion University. He is an industrial technology program leader. He received his EdD in Technology Education from North Carolina State University in 2007, his MEd in Technology Education from California University of Pennsylvania in 2004, and his BS in Industrial Technology from California University of Pennsylvania in 2003. His research focuses on improving teacher and student performance in STEM education and enhancing the development of a national STEM-educated workforce. Dr. Katsioloudis may be reached at pkatsiol@odu.edu

LINDA VAHALA received her BS degree from the University of Illinois in 1969, MS degree from the University of Iowa in 1971, and PhD from Old Dominion University in 1983. Her publications include articles in both plasma physics and atomic physics with an emphasis on laser interactions with plasma and with neutral/rare gas collisions. She has presented her work at various international workshops and meetings, both in Europe and in the United States. She is an associate professor of electrical and computer engineering at ODU. In 1995, she received the Peninsula Engineer of the Year award. Dr. Vahala may be reached at lvahala@odu.edu

HONQUI (MICHAEL) WU is the Batten Chair of Cybersecurity and the Director of the Center for Cybersecurity Education and Research at Old Dominion University. He is also a professor in the Department of Electrical and Computer Engineering. He received his BS degree in scientific instruments from Zhejiang University, Hangzhou, China, in 1996, MS degree in electrical engineering and PhD degree in computer science from the State University of New York at Buffalo in 2000 and 2002, respectively. His research focuses on networked cyber-physical systems for security, safety, and emergency management applications, where the devices are often lightweight, with extremely limited com-

puting power, storage space, communication bandwidth, and battery supply. Dr. Wu may be reached at h1wu@odu.edu

DEBORAH K. MARSHALL is a career and technical education teacher specialist for the Norfolk Public Schools. She received her degrees from Longwood College, Old Dominion University, The George Washington University, and Regent University. In the Norfolk Public School system, she has worked as an instructional technology resource teacher, CTE teacher, and served as Department Chair of CTE at Granby High School. Previously, she worked for Gloucester County Public Schools as a middle school CTE business teacher. Throughout her time in CTE, she has served on curriculum writing committees for the Virginia Department of Education. Deborah Marshall may be reached at dmarshall@nps.k12.va.us

MICHAEL ANTHONY CRESPO is the department chair for career and technical education at Granby High School, Norfolk Public Schools. He teaches AP computer science principles, cyber security fundamentals, and cyber security software operations Code.org and codevirginia.org and is the Computer Science Discoveries Facilitator. Mr. Crespo may be reached at mcrespo@nps.k12.va.us

MARY ADDISON works as an executive assistant to the dean and instructional designer for Batten College of Engineering and Technology. She holds an MS in Business and Industry Training and BS in Occupational and Technical Studies (Training Specialist) from Old Dominion University. Mrs. Addison may be reached at maddison@odu.edu