2020

INNOVATIONS IN CYBERSECURITY EDUCATION

NATIONAL
CYBERWATCH
CENTER

NATIONAL CYBERWATCH CENTER 2020 Innovations in Cybersecurity Education
National CyberWatch Center Digital Press ID *NCC-2020-INNOVATION-01*
https://www.nationalcyberwatch.org/innovations

Table of Contents

01. EVIDENCE-BASED STRATEGIES

02. INSTRUCTION

Table of Contents

03. PRACTICE

04. PROGRAM DEVELOPMENT

Message from the Director

One of the major strengths of the National CyberWatch Center is its ability to aggregate and disseminate the capacity and creative experimentation found within our academic and workforce communities. The 2020 Innovations in Cybersecurity Education publication is an example of this strength in action.

The Innovations in Cybersecurity Education program, part of our awards and recognition project, was built on the premise that our members are some of the best cybersecurity educational innovators, and that through our Center, they can share their innovations, accelerate their adoption, and receive proper recognition for their work.

In the first two years of the program (2017, 2018), all submissions were included in the final publication. In last year's Innovations program, we emphasized quality over and quantity and the same goes for this year as well. In total, 53 submissions were received (up from 47 in 2019), of which 40 were chosen for this year's publication and dissemination efforts in the following categories: Evidence-Based Strategies, Instruction, Practice, and Program Development.

For the fourth year in a row, this reference document was created listing all the accepted submissions, with a brief write up for each. In addition, a wrap-around social media campaign will promote the winners and select submissions as a way to circulate these innovative and effective practices to a larger audience. Lastly, this year's winners and those recognized as Honorable Mention submissions, will be honored during the opening virtual plenary at the 2020 Community College Cyber Summit (3CS) on August 4 from 6-8pm ET.

I want to thank those who submitted this year. I also want to acknowledge and thank those that served on the Review Panel for their hard work. They include past winners, distinguished professors, leaders in cybersecurity education and workforce development, and those on the front lines educating the next generation of information security professionals.

I hope you are able to glean some "nuggets" from the extraordinary work showcased in this publication. I also hope you can implement some of these effective practices in your programs.

Best regards,

Casey W. O'Brien
Executive Director & Principal Investigator
National CyberWatch Center

01

EVIDENCE-BASED STRATEGIES

WINNING SUBMISSION:
A CYBERSECURITY STRATEGY FOR AT-RISK YOUTH

A CYBERSECURITY STRATEGY FOR AT-RISK YOUTH

WINNER

EVIDENCE-BASED STRATEGIES

DESCRIPTION

After two years of comprehensive studies (PACE, http://bit.ly/innovation-2019) at Cypress College to develop Cybersecurity pathways from middle school all the way to College, we realized that despite all the successes, it did not address the at-risk youth population. Ironically, the latter is the "population" most likely to choose community college over 4-year schools due to the background and income levels of students. Accordingly, we implemented a strategy for a pilot Cybersecurity program addressing at-risk youth entering college.

During Spring and Summer of 2019, we developed a partnership with the Sunburst Youth Challenge Academy to collaborate with their Job Challenge program. The mission of the Sunburst Academy is: "To intervene in and reclaim the lives of 16-18 year old high school dropouts, producing program graduates with the values, life skills, education, and self-discipline necessary to succeed as productive citizens" (https://sunburstyouthacademy.com). Formed by the National Guard, California Jobs Challenge is a 22-week residential career technical academy exclusively for California Youth Challenge graduates. The program provides post-secondary career technical education (CTE), training, and career readiness skills leading to foreseeable employment. The main objective of the program is to make at-risk youth educated and "job ready."

Following several meetings with the Jobs Challenge supervisors, 25 at-risk youth were assigned to Cypress College for one semester of Cybersecurity education. It was a compressed schedule where students attended class Monday through Thursday from 9 am to 1 pm, followed by 2 hrs. of lab and tutoring sessions in the afternoon (2-4 pm). During Fridays, students went through career counseling to develop their soft skills including interview skills and resume building and participated in field trips and Cybersecurity competition events. Care was taken to provide as much resources as possible for this program to ensure an engaging, encouraging and supportive educational environment. Two full-time faculty members, three college mentors, one lab assistant and several counseling/dual enrollment staff were involved in the process. Out of the 25 students, 23 completed our Centers of Academic Excellence in Cyber Defense (CAE-CD) program of study which included four Cybersecurity courses.

All 23 students obtained our Cybersecurity College certificate. 16 students passed CompTIA's ITF+ industry exam, seven students passed CompTIA's Cloud Essentials exam and two students passed CompTIA's Security+ exam. Four students interviewed with the Sybsync IT company for a paid internship program and will start the internship in Spring of 2020. The same four students shared their experience in a presentation at the ICT-Educators conference in San Jose in January 2020. By far the most positive and heartfelt outcome of our pilot study was observing the transformation of students from uncertain, skeptical and dejected individuals to confident, optimistic and cheerful ones.

BENEFITS

- A compressed Cybersecurity education program designed for at-risk youth that follows our CAE-CD program of study
- Opportunity for at-risk youth to complete a college certificate in one semester
- Opportunity for at-risk youth to pass several industry certificate exams in one semester
- Opportunity for at-risk youth to develop their soft skills (i.e. resume writing, interview)
- Opportunity for at-risk youth to enter into a paid internship program
- Empowering at-risk youth to share their experience by presenting at a conference
- Overall transformation of students from a hopeless to a positive and hopeful state

CONTACT INFORMATION

Behzad Izadi

bizadi.cypress@gmail.com

Cypress College

02

INSTRUCTION

WINNING SUBMISSION:
GIRL SCOUTS LEARN WHAT IT TAKES FOR AN INCIDENT RESPONSE TEAM

GIRL SCOUTS LEARN WHAT IT TAKES FOR AN INCIDENT RESPONSE TEAM

WINNER

INSTRUCTION

DESCRIPTION

The Girl Scouts Cyber Challenge is Girl Scouts of the USA's first-ever national STEM challenge event, developed and sponsored by Raytheon. On October 19, 2019, thousands of girls across 10 U.S. cities solved a hypothetical ransomware attack on a moon base, cultivating key cybersecurity skills with support from Raytheon volunteers and mentors.

Girl Scouts of Historic Georgia was one of ten councils selected to pilot the Cyber Challenge event, thanks in part through generous support from Raytheon. In recognition of October as National Cybersecurity Awareness Month, the Cyber Institute at Augusta University's School of Computer and Cyber Sciences took this great opportunity to be a catalyst, partner, and host for this event. Over 125 Girl Scout Cadettes, Seniors, and Ambassadors, (girls ranging from 6th-12th grades), as well as 25 troop leaders from across the state of Georgia participated in this inaugural event at the Georgia Cyber Center in downtown Augusta, Georgia.

Augusta University and Augusta Technical College classrooms were transformed as stations, where Girl Scouts were enlisted to help with a hypothetical hack that occurred on a moon colony. Participants were part of an incident response team that must find out who hacked the system and how to stop them. Details and materials were developed months before the event by Raytheon and information webinars were conducted with Girl Scout staff and members from each council outlining the plan to ensure a successful implementation. The Challenge activities were designed as "plugged" and "unplugged" stations for up to 20 girls to rotate thru each station. Girls were introduced to the Moon Base scenario playing the role of being onboarded to their new positions on the Moon Base. Each girl was given Investigation files, and a Cybersecurity Field Manual, which included common cybersecurity terms and was used to guide them as they solved the challenges at each Station. Girls learned that the Moon Base had a serious cybersecurity breach and it was up to their "incident response teams" to investigate the attack. While some of the activities were a learning stretch depending on the girl's age and technology experience, all girls were introduced to cryptography techniques, cybersecurity investigation procedures, phishing, and incident response procedures. If teams were stuck on an assignment and needed help, they were given a coin to request up to three consults at each Station. At the end of each Station, girls reported their findings on their team Incident Response Data log and certificates were awarded at the end of the day based on how many flags were entered correctly into the Investigation Database.

BENEFITS

As a Center of Academic Excellence in Cyber Defense, Augusta University seeks opportunities for outreach in cybersecurity education. Partnering with the Girl Scouts is a smart choice for the university community to introduce more girls to the STEM and cybersecurity fields. The Girl Scout Cyber Challenge, held in the Georgia Cyber Center was a perfect space to hold the event, giving the girls a glimpse of a "real-world" experience in a facility designed for teamwork. The Georgia Cyber Center is a unique public/private collaboration among academia, state, federal and local government, law enforcement, the U.S. Army and the private sector. With two adjacent buildings totaling 332,000 square feet, the Georgia Cyber Center, located on the Nathan Deal Campus for Innovation, is designed to meet the growing need for cybersecurity talent in Georgia, the nation and across the globe.

CONTACT INFORMATION

Karen Ribble

kribble@augusta.edu

Augusta University

STOQ-SRA: A SELF-LEARNING TOOL OF QUANTITATIVE SECURITY RISK ASSESSMENT

HONORABLE MENTION

INSTRUCTION

DESCRIPTION

The assessments of the security risks of the buildings that house hardware and software, the hardware and devices that house data and run application programs are important to the survival of any enterprise. The risks of security threats from virus, thefts, hackers, natural disasters, and various attacks must be carefully identified. An enterprise ought to weigh the annualized loss expectancy due to each vulnerability against the cost of providing safeguards. The accreditation of Cybersecurity programs by the Accreditation Board of Engineering and Technology (ABET) requires students to learn and demonstrate the knowledge of risk assessments. Case-based security risk assessment learning and practice modules should be predicated on reliable models such as, The 2018 Security Management Framework by National Institute of Standards and Technology (NIST). The learning modules should relate the security risk assessment scenarios to the requirements of NIST for security risk management. The practice modules should provide practical hands-on risk assessment exercises based on NIST requirements of risk management for enterprises. Following the NIST requirements, the variables in a security risk assessment model can be rated on a continuous or categorical scale. With too many variables, the quantitative data analysis of the security risk assessments can be cumbersome. Consequently, the tool called STOQ-SRA with a graphical user interface was designed and implemented to facilitate self-learning of data-driven quantitative and qualitative security risk assessments.

BENEFITS

Cybersecurity students need to learn the formal models and methods of security risk assessments. Students can use the tool, STOQ-SRA, to identify risks of security threats from virus, thefts, hackers, natural disasters, and various attacks; to weigh the annualized loss expectancy due to each vulnerability against the cost of providing safeguards; and to solve case-based and scenario-based quantitative security risk assessment problems. Students can use the graphical user interface tool for self-paced learning of security risk assessments. Instructors can use the tool to design practical hands-on case-based projects for teaching and learning of security risk assessments.

CONTACT INFORMATION

Amos O. Olagunju & Hari G. Shrestha

aoolagunju@stcloudstate.edu

St. Cloud State University

ASSESSMENT STRATEGIES IN CRYPTOGRAPHY & CRYPTANALYSIS COURSE

INSTRUCTION

DESCRIPTION

Foundations of Cryptology is an introductory course on cryptography and cryptanalysis at Boise State University. The main focus of the course is on definitions, theoretical foundations, and proofs of security, with programming practice. Topics include symmetric and public-key encryption, security analysis, message integrity, hash functions, digital signatures and fundamentals of number theory.

The course is focused on hands-on work in an interdisciplinary environment and using computational/algorithmic tools. The innovation presented in this submission features some of the assessment methods that I have developed and used in this course for the past several years:

- The quizzes in this course are team-based and hands-on. The goal of this component of the course is to simulate the real-world practice of cybersecurity, where teams of people with different backgrounds contribute to the common objective of analyzing and solving a cybersecurity problem
- The final exam is an individualized take-home test. It is posted online (via Blackboard), and it is due within one week from the date of posting. A few days prior the start of the final exam each student has to send me their public-key (e.g. RSA key) via email. A single (randomly chosen) message per submitted public key is encrypted using that public key. Public-key (or asymmetric) cryptography uses two different keys: one of the keys (the public key) is available to everyone and the other key (te private key) is confidential to its respective owner. Data encrypted with the public key can be decrypted with only the corresponding private key
- The list of students' public keys (and not the corresponding students' names), the list of encrypted messages (ciphertexts), and the list of individualized exams are posted online (via Blackboard). Blackboard is the primary Learning Management System (LMS) used for online and web- assisted courses at Boise State University. Access to a course website in Blackboard is restricted and is available only to the students enrolled in the class. Each of the above mentioned three lists is enumerated. The numerical order of items appearing in one list is unrelated to the numerical order of items in the other lists
- Each student determines which of the posted exams the student is responsible for by identifying the list number of the ciphertext is decryptable using the student's private key: the number of the ciphertext message decryptable by a student's private key is the number of the test the student is responsible for
- The final exam has points reserved for key-security and the remaining points are for actual work handed in
- All public-keys are open to attack by the students enrolled in the class. Any student, who during the week of the final, successfully determines the private key corresponding to a posted public key other than their own and is among the first two to sufficiently report this accomplishment to the instructor, will earn extra credit points
- Proof of successfully determining a private key consists of submitting (via email) the discovered private key, plus the decryption of the posted ciphertext associated with that private key
- The information about which public-key was successfully attacked during the exam week is not available on the course website and not revealed to the class
- Note that although a student enrolled in the course may successfully attack any number of posted public keys, earning extra credit points for each successful attack, that student is still required to complete and submit their own final exam

BENEFITS

The innovation featured in this submission offers assessment methods that blends conceptual/theoretical aspects of cybersecurity with practical applications. Moreover, the course design format provides an opportunity for development of teamwork skills, and apply concepts learned in class through critical thinking and problem solving.

CONTACT INFORMATION

Liljana Babinkostova
liljanababinkostova@boisestate.edu
Boise State University

EXPERIENTIAL USE OF RASPBERRY SBC TO DETECT COUNTERFEIT INTEGRATED CIRCUITS

INSTRUCTION

DESCRIPTION

An inexpensive single board computer offers a useful tool to offer learners insights in Internet of Things devices, circuits, networks and supply chains. Experiential uses offer an effective way to consider computer architecture's integrated circuits in conjunction with critical thinking constructs of identification, characterization and comparisons. The innovation builds on forensics and systems resilience construction.

BENEFITS

Critical thinking, process checklists, systems architecting, experiential learning, supply chains and counterfeit ICs.

CONTACT INFORMATION

Larry Leibrock
larry.leibrock@inl.gov
Idaho National Lab

EDUCATING THE MASSES: CYBERSECURITY EDUCATION FOR EVERYONE

INSTRUCTION

DESCRIPTION

To help build a cybersecurity talent pipeline, Norfolk State University hosted the 2019 GenCyber Summer Professional Development Workshop for High School Teachers. The purpose of this one-week professional development workshop was to introduce a curriculum that high school STEM teachers and other interested teachers could use to introduce the GenCyber concepts in their classrooms in a fun and engaging approach. The teachers received instruction in designing lesson plans associated with GenCyber concepts. They designed lesson plans and activities based on what would integrate best into their curricula. For example, the participants were engaged in paired sessions of scripted play scenarios where one person was the hacker and the other was the victim. A packet sniffing tool (Wireshark) was used to demonstrate how information is accessed by hackers and how participants can improve their security to prevent attacks such as unauthorized access to information or modifying information sent to someone else. The participants were introduced to cryptography and cryptographic systems and exposed to several cipher techniques and engaged in hands-on sessions that allowed them to experience real-world data security issues. The activities included utilizing the Virginia Cyber Range, hands-on experiences, interactive lectures, guest speakers, career exploration, and textbook showcases.

BENEFITS

The benefits of the innovation were providing active learning opportunities and knowledge in how teachers can acquire the skills to complete a final learning product that can be utilized immediately when they return to their classroom. Another benefit was that the GenCyber course was professionally designed and developed by a Quality Matter Peer Review and Blackboard MVP with the intent to have a significant online component, thus providing continuous support, resources, and updates for the participants throughout the school year. This benefit fostered community building, learning, and ensured that information was shared beyond the workshop. The online resource component helped to connect all participants, teachers, and instructors before, during, and after the workshop. All lesson plans that were created were uploaded in the repository for availability. Few schools in the K-12 sector are developing curriculum related to cyber awareness about the security risks of online behavior.

The new innovative approach provided an ideal collaboration and opportunity to educate teachers and students between higher education and K-12. It is critical that all students receive education that deepens their conceptual and practical understanding of issues and awareness in cybersecurity education. By offering this innovative approach the masses learned how to better protect their information and improve their behavior from a cybersecurity and privacy standpoint. Society at large benefits by: (1) increase interest in cybersecurity education to attract high school students to contribute to the USA's efforts to increase the number of cybersecurity professionals in the workforce, (2) improve teaching methods to enable teachers to effectively facilitate content for K-12 curricula and to become advisors and mentors to students interested in the field, (3) collaborate with high school teachers to assist in recruiting students with an interest in computer science and cybersecurity into Norfolk State University's Computer Science and Cybersecurity programs.

CONTACT INFORMATION

D'Nita Andrews Graham

dagraham@nsu.edu

Norfolk State University

SECURITY OPERATIONS CENTER-BASED (SOC) ANALYST EXPERIENCES

INSTRUCTION

DESCRIPTION

Capitol has built a student run security operations center (SOC) experience into our BS cybersecurity program. Students volunteer to train for tier 1 SOC analyst skills within the SOC gaining experience and certifications on Splunk and Alien Vault. The students are enrolled in a self-paced course housed on the Cybrary platform. At the end of the 6-month sprint, as it is called, students gain industry recognized certifications, training and experience, which employers have validated.

BENEFITS

- Students are better prepared for internships and employment
- Students gain valuable certifications
- Student gain valuable experiential learning within the SOC
- Student knowledge in related courses is increased
- Employers gain students with more advanced skills
- Students gain situational awareness of threat detection and incident response

CONTACT INFORMATION

William Butler
whbutler@captechu.edu
Capitol Technology University

STRATEGIC CYBER SECURITY STUDIES

INSTRUCTION

DESCRIPTION

Cybersecurity education requires a multi-disciplinary approach to best support positive learning outcomes. Successful engagement with the discipline requires not just technical competencies in areas such as coding, networking and hardware, but also an understanding of the geo-political, socio-cultural, and psychological issues relevant to the field. With this in mind, Augusta University's School of Computer and Cyber Sciences, in conjunction with AU's Department of Political Science, created the following two innovative courses: "Introduction to Strategic Cybersecurity," and "Cyber Conflict: History and Theory of Cyber War."

BENEFITS

The benefit of these courses is that it helps traditional CS students place their studies into a greater, global context. They will have a better understanding of the strategic cyber threats posed by nation-state actors (specifically, Russia, China, Iran and North Korea) as well as an understanding of how these actors developed, organized, and have used their cyber capabilities against the United States.

CONTACT INFORMATION

John Heslen
jheslen@augusta.edu
Augusta University

PROVIDING THOROUGH, ECONOMICAL COURSE MATERIALS FOR STUDENTS

INSTRUCTION

DESCRIPTION

In order to provide an abundance of course materials for Cybersecurity students, Hill College utilizes Cengage Unlimited, which offers a digital subscription that provides students TOTAL AND ON DEMAND ACCESS to all the digital learning platforms, eBooks, online homework, lab/simulations/scenarios and study tools. We are a small and rural institution, therefore cognizant of student costs.

BENEFITS

Student investment is less than $120 each semester for all courses, while instructors can provide assignments and training materials from several textbooks in each class. Often times, providing a different author’s explanation or exercise aids the learning process. Multiple resources provide exposure to important, but less emphasized topics. With the savings, we are currently reviewing VR training platforms that provide real world attacks that our students could afford to purchase.

CONTACT INFORMATION

Jackie Armstrong

jac@hillcollege.edu

Hill College

A VIDEO-BASED CYBERSECURITY MODULAR LECTURE SERIES FOR COMMUNITY COLLEGE STUDENTS

INSTRUCTION

DESCRIPTION

Building from our experience collaborating with Hagerstown Community College, The Johns Hopkins University Information Security Institute has developed a distributable course of video lectures aimed at community college students. The course is composed of four modules: 1) offensive security and digital forensics, 2) the Internet of Things, 3) cryptography, and 4) blockchain technologies. Each module is composed of three or four video lectures with a total of thirteen lectures. The lectures are delivered by JHU faculty, graduate students, and staff. Each lecture video is accompanied by supporting materials including exercises for the students that can either be used as homework or in-class assignments. Many of the exercises can be used as laboratory exercises. The exercises are designed with a broad range of student ability in mind and can be used to develop a tailored experience that meet the needs and abilities of most students. We also believe the lectures may be of use to advanced or interested high school students.

Thanks to input from local community college faculty, the course has been designed to be put to use in numerous ways including, as a course for credit, a seminar series, individual standalone lectures or modules, and for use as content to complement existing curriculum. The course is available at no cost to anyone who requests it via the website cybercourse.isi.jhu.edu. This work was supported by NSA CNAP Award #S004-2017.

BENEFITS

There is a shortage of cybersecurity workers. We developed this lecture series as a way to increase interest in the field of cybersecurity and to attract more students to the field. Students viewing all of the lectures are exposed to a broad range of topics in cybersecurity including cryptography, password cracking, unmanned aerial vehicle hacking, blockchain, and more. We designed the materials to be as modular as possible though there are some prerequisite relationships between some of the lectures, so the material should be accessible to anyone.

CONTACT INFORMATION

Joseph Carrigan
joseph.carrigan@jhu.edu
Johns Hopkins University Information Security Institute

SECURE SCRIPTING: AN OER TO TEACH CYBERSECURITY CONCEPTS USING BEST PRACTICES IN PROGRAMMING

INSTRUCTION

DESCRIPTION

Secure scripting is now considered one of the pillars in the cybersecurity curriculum. Many academic programs across the nation, in both, two/four-year colleges, have learning outcomes/objectives aligned to secure scripting-related concepts. There are numerous books on scripting, programming, Linux or cybersecurity itself. However, often it is quite challenging to find a resource that compiles all these in one place, contextualizing concepts towards cybersecurity practice.

We present an Open Educational Resource (OER) called "Secure Scripting" (sites.google.com/site/securescripting), that provides an introduction to Linux, followed by a gentle introduction of secure coding principles and practices using sample scripts. Finally, we use Introduction to Python, as one of the most required programming languages nowadays in the industry.

BENEFITS

- Material available to use and adapt to the classroom: instructors can use the material provided in this repository to incorporate in any secure scripting course. New versions of the OER are updated based on material provided by other contributors
- Original practices in programming: all the practices in the repository are original and are posted for dissemination purposes. Any variation of these practices is also listed on the site
- Grading Rubrics based on learning outcomes: rubrics for programming practices are provided based on Bloom's taxonomy of learning outcomes
- Alignment to curricular guidelines and standards: materials list the alignment to ACM Curricular Guidelines, 2019 CAE Designation Knowledge Units, and the NICE framework
- Scenarios and Projects Repository: a Project-Based Learning (PBL) list of projects to assist courses that adopted this format

CONTACT INFORMATION

Christian Servin

cservin1@epcc.edu

El Paso Community College

USING SOCIAL ROBOTS TO INNOVATE SECURE CODING EDUCATION

INSTRUCTION

DESCRIPTION

This cyber educational innovation is based upon a novel instructional module and strategy that focuses on teaching software security to students using a social robot - Cozmo. It consists of a unique Cozmo robot based secure-coding lesson-plan, as a new experiential-learning model, which combines learning of software security concepts with educational-robotics (ER) in the form of hands-on, interactive Cozmo secure coding. We have preliminary evidence of the effectiveness and potential of our experiential-learning approach as a more enhanced and engaging medium for learning software security via defensive programming of Cozmo.

BENEFITS

- To our knowledge, this is the first-of-its-kind approach towards educational innovation in teaching secure coding using Cozmo
- This fresh experiential learning model fills a gap in cyber education, based upon existing literature
- It innovates and enhances traditional secure coding instruction and learning, which involves no ER
- It demonstrates vulnerabilities in programming of a Cozmo robot
- The learning assessment data gathered through our innovation project can help in showing that our approach of involving ER in the form of social robots, like Cozmo, can improve the traditional techniques of teaching secure coding

CONTACT INFORMATION

Ankur Chattopadhyay
profachattop@gmail.com
Northern Kentucky University

CYBER COMPUTER SCIENCE PRACTICES: A CYBERSECURITY-BASED CURRICULUM FOR THE CS FIELD OF STUDY

INSTRUCTION

DESCRIPTION

With the double objective of satisfying regional workforce/industry needs in cybersecurity work positions and to assist students to complete an A.A./A.S. in CS and then transfer into a CS program in a four-institution with a cybersecurity concentration, we propose cyber-computer science: a set of real-world cybersecurity programming practices that permit students to program with adversarial thinking in mind. The two-fold purpose of these practices is:

1. To infuse cybersecurity concepts into two-year degrees in Computer Science and
2. To enhance the Knowledge, Skills and Abilities (KSA) based on the NICE framework into two-year degrees

A set of programming practices in the Computer Science Field of Study (FOS) (i.e., CS 1, 2, 3 and Computer Organization and Machine Language) covers programming practices with the intention of learning Computer Science principles applied to cybersecurity concerns.

BENEFITS

- To associate learning outcomes from ACM Computer Science Curricular Guidance for associate-degree transfer programs with infused cybersecurity into the curriculum of the first two years of CS education
- To associate competencies and learning outcomes from the ACM Curriculum Guidance for two-year cybersecurity programs
- To Identify tasks, knowledge, skills, and abilities for Computer Science work roles based on the NICE Framework work roles. Particularly, in the case of Computer Science, the practices are intended to satisfy positions that involve software development
- To cover topics that satisfy outcomes based on the DHS/NSA CAE guidelines. Many colleges designated CAE course's outcomes/ knowledge areas must be mapped to the CAE Cyber Defense 2019 Knowledge Units
- To cover content for fundamentals in cComputer Science, which in many cases, corresponds to the Field of Study (FOS) that is established in many institutions as an A.A. and A.S. in Computer Science.

CONTACT INFORMATION

Christian Servin

cservin1@epcc.edu

El Paso Community College

CLARK HOSTS THE LARGEST COLLECTION OF FREE QUALITY CYBERSECURITY LEARNING OBJECTS TO BE USED BY ALL FACULTY TEACHING CYBERSECURITY

INSTRUCTION

DESCRIPTION

Clark hosts the largest collection of free cybersecurity curriculum created by top-researchers and peer-reviewed by instructional designers and subject matter experts. It contains over 700 learning objects, ranging from nano-modules (less than 1 hour) to full courses that address critical cybersecurity topics, all under the Creative Commons license.

BENEFITS

The global cybersecurity crisis needs impactful solutions. Clark provides an innovative model for the design, adoption, reuse and remix of high-value cybersecurity curriculum. The Clark cybersecurity curriculum development model culminates in high-impact learning objects designed by research experts in concert with instructional designers. The Clark system’s novel features include: Bloom’s taxonomy-based assistance for content creation, mapping to prominent curriculum guidelines, and a faceted search. By providing access to modular curriculum, ranging from fundamental cybersecurity concepts to cyber law, cyber-physical systems, blockchain, and quantum cryptography, Clark will better prepare the cyber-workforce and raise the baseline of students to perform critical research.

CONTACT INFORMATION

Blair Taylor
btaylor@towson.edu
Towson University

10 TOPICS IN FIVE ONE-DAY SEMINARS

INSTRUCTION

DESCRIPTION

We are offering a certification in Cyber Intelligence. A one-day seminar is given every other month. During that one-day seminar two topics are presented, discussed and learned. Certificates of completion are given for the two subjects completed during a seminar. After a student attends five seminars (ten subjects) they are Cyber Intelligent Certified.

BENEFITS

Most people cannot dedicate a full five days to educational programs and seminars, so we adapted to their needs. Although they are dedicating five days to the process of becoming Cyber Intelligent, it is done over a ten-month period. This process does not overwhelm the student and they have time to prepare for the next two subjects.

CONTACT INFORMATION

Dean Lane
dlane@iwp.edu
The Institute of World Politics

COMPETENCY-BASED CAPSTONE COURSE USING NICE CHALLENGE AND NCL COMPETITION

INSTRUCTION

DESCRIPTION

The Capstone course is designed to give the student an understanding and measurement of the knowledge they have acquired over the completion of the Information Systems Cybersecurity Degree and Computer and Network Security Certificate programs. The course allows students to apply that knowledge and understanding by participating in the National Cyber League (NCL) capture the flag cyber challenges and using the NICE Challenge, and the proactive gymnasium and labs to prepare for the competition and jobs. The NICE Challenges provide students and faculty an assessment of students' knowledge, skills and abilities in NICE Operate and Maintain and Protect and Defend job roles.

BENEFITS

- Provides students with assessment of their hands-on job skills and abilities as simulated in the NICE Challenges and NCL challenges
- The NCL promotes their soft and hard skills in teamwork, communications, and trouble-shooting abilities
- The NCL provides a Scouting Report that may be shared with future employers' interviews and on resume
- Students have experienced job placement success based on the understanding of the NICE Framework job roles and where they excel in those job roles
- The faculty and student collaboration in improving the overall Information Systems Cybersecurity Curriculum
- Provides faculty with student knowledge, skills and abilities performance measurements to promote continuous improvement in all the courses leading up to the Capstone course

CONTACT INFORMATION

Stephen Miller

stephen.miller@enmu.edu

Eastern New Mexico University-Ruidoso Branch Community College

THE “STORY” OF NETWORK SECURITY

INSTRUCTION

DESCRIPTION

Instruction that “tells a story” across a semester can capture the minds of students, encourage attendance, and passion for the topic. When I was asked to take over our network security and cryptography class, I decided to take that approach.

The semester starts with a preface: I provide some background on cybersecurity (the CIA’s), networking, and ethical/legal issues that the course will encounter. From here, the story of network security starts with the human component: who commits crimes and why, and how social engineering is a common strategy. From here, I ask the question, what is the most common way that users interact with a network (the answer is their browser)? We then dive into browser specific security. The next question is, when you are browsing the web, where does that content come from, and the answer is servers, facilitated by networks. We then start with observing what we can run on servers via port scanning and enumeration. From here, we move into vulnerabilities, exploits and attacks utilizing Metasploit, and then finish out or discussion with a discussion of web development vulnerabilities. As a bit of prologue, we introduce cryptography, tying it back into the entire story of network security as told to that point.

Since structuring the class in this manner, it has become one of the most popular classes in the department, nearly filling our largest computer lab.

BENEFITS

Instead of teaching the class as an amalgamation of ideas and topics, the “story” connects each series of lectures in a way that students can connect with. I find that organically, attendance is much higher in this class, and students will even tell me “I just don’t wanna skip this class, it is really interesting.”

As an added benefit, cryptography is often intimidating to many students. I find that telling the story of network security, and then in the end saying “remember all these problems we talked about,” here is why cryptography is important and what it can do to help really piques their interest in the topic.

CONTACT INFORMATION

Christopher Kreider
chris.kreider@cnu.edu
Christopher Newport University

CYBERROLL

INSTRUCTION

DESCRIPTION

CyberRoll is a role-play focused cybersecurity board game. The game teaches and promotes cybersecurity program development and management, communication, and resource planning.

BENEFITS

Cybersecurity students are exposed to real-world cybersecurity response, security control deployment and configuration, defense strategies, program planning, financial planning. communication planning, and group interaction before entering into the cybersecurity job market.

Benefits also include student preparedness for security certifications, and improved test scores in ISIN 308 at Ferris State University.

CONTACT INFORMATION

Molly Cooper
mollycooper@ferris.edu
Ferris State University

DEVELOPMENT OF A GRADUATE-LEVEL RESEARCH METHODS COURSE IN CYBERSECURITY

INSTRUCTION

DESCRIPTION

The North Dakota State University launched a new Research Methods in Cybersecurity course in 2019. This course brings together the research method components of multiple disciplines that are related to cybersecurity into a single course that graduate students with an interest in cybersecurity can take to prepare for their research. An interdisciplinary course such as this was needed as many of the most pressing cybersecurity research challenges span disciplines and require the use of research methods from multiple domains. While the course obviously doesn't cover every facet of how to perform research across numerous areas, it provides an introduction to many different disciplines' research paradigms, tools and approaches - and explains how they can be connected. Students can pursue additional research into areas that may be most relevant to their research areas. In addition to learning about the different research methods, students participated in a discussion board where they learned about current cybersecurity research in multiple sub-fields and completed a research project.

BENEFITS

The principal benefit of this innovation is that it fills a gap that existed in NDSU's curriculum and exists at many other institutions. Students that complete this course have a holistic knowledge of how research can be conducted across the entire broad and multi-disciplinary range of cybersecurity-relevant fields.

CONTACT INFORMATION

Jeremy Straub
jeremy.straub@ndsu.edu
North Dakota State University

03

PRACTICE

WINNING SUBMISSION:

SITUATIONAL & CYBERSECURITY AWARENESS FOR PUBLIC HEALTH RESEARCHERS

SITUATIONAL & CYBERSECURITY AWARENESS FOR PUBLIC HEALTH RESEARCHERS

WINNER

PRACTICE

DESCRIPTION

Over the past decade, many public health research efforts have been including information technologies such as Mobile Health (mHealth), Electronic Health (eHealth), Telehealth, and Digital Health to assist with unmet global development health and problem needs. This innovation includes background on the documented lack of Cybersecurity risk or vulnerability assessments taking place in global public health research, areas where greater assessments are taking place and existing frameworks and policies that may be adopted. In addition, a proposed research paper section could be utilized to help minimize Cybersecurity and information security risk.

BENEFITS

This innovation brings about critical Cybersecurity awareness to those individuals involved in public health research efforts that include a technology component via mHealth/eHealth and Digital Health. This innovation was initially introduced in a research publication earlier in 2019 and recently further developed at Kean University via a research publication. This innovation brings about a toolbox and concept that global public health researchers can utilize to help them implement technologies with greater Cyber knowledge.

CONTACT INFORMATION

Stanley Mierzwa
smierzwa@kean.edu
Kean University

CYBERSECURITY FOR ALL

HONORABLE MENTION

PRACTICE

DESCRIPTION

Cybersecurity for All is an innovative program designed to address the critical shortage of qualified cybersecurity professionals via competency-based education and hands-on skills development. It helps individuals launch or advance a career in cybersecurity, and re-skill, up-skill or earn industry certifications for evolving cybersecurity roles. Cybersecurity for All is an agile program that offers short courses on cutting-edge topics that blend higher education best practices and competency-based hands-on skills development.

Cybersecurity for All addresses the national cybersecurity workforce crisis by preparing individuals for evolving cybersecurity work roles from day one on the job and supporting organizations' needs for flexible, ongoing education to enhance cybersecurity workforce readiness.

Program Goals:

- Increase the number of qualified cybersecurity professionals
- Enhance readiness and competencies for evolving cybersecurity work roles
- Help individuals launch or advance cybersecurity careers
- Help organizations train, re-skill or up-skill personnel for evolving cybersecurity roles, including federal, state and local government, defense and private sector organizations

BENEFITS

Since the program was launched, over 25 courses have been developed and offered to over 700 participants. The courses have been offered to personnel from all 47 Florida State Agencies in partnership with the Florida Department of Management Services, and to Supervisors of Elections and IT personnel from all 67 Florida Counties in partnership with the Florida Department of State. In addition, the courses have been offered to the general public, small businesses, defense organizations and veterans.

Program Benefits:

- Evolving topics to address emerging cybersecurity work roles, including incident response, cloud security, threat intelligence, threat hunting, network defense, industrial control systems security, malware analysis, risk management and secure software development
- Integrates best practices in higher education with hands-on skills development using the Florida Cyber Range, a state-of-the-art virtual environment. Realistic scenarios and exercises are integrated into all courses using the Florida Cyber Range to create authentic learning experiences and enhance competencies
- Courses are modular, stackable and customizable for organizations. For example, courses offered to Florida State Agency personnel were customized to include the Florida IT Security Rule in addition to NIST and other national best practice guidelines

- Courses align with the NIST NICE Cybersecurity Workforce Framework (NCWF). Each course identifies the NCWF work roles and the Knowledge, Skills and Abilities (KSAs) that it prepares individuals for
- Provides continuing education credit (CEUs/CPEs) as well as potential credit toward academic degrees and certificates
- Courses can be delivered face-to-face, online or remotely

CONTACT INFORMATION

Eman El-Sheikh
eelsheikh@uwf.edu
University of West Florida

BUILDING AND HACKING AN EXPLOITABLE WIFI ENVIRONMENT FOR YOUR CLASSROOM

PRACTICE

DESCRIPTION

With the modern widespread use of WiFi, it is important to demonstrate how WiFi access points can be exploited in practice due to design weaknesses. The theory behind exploiting WEP and WPA2 has been available for a number of years. However, it has not been easy to practice how these theories get applied in a real environment.

Offering learners the opportunity to have hands-on experience in hacking WiFi access points is challenging, especially in a classroom setting. This is due to the fact that there are so many variables to be considered in order to provide learners with a seamless experience and allow educators to focus on learning outcomes rather than spending an unreasonable amount of time troubleshooting problems.

This innovation allows educators to learn how to build and configure WiFi access points for learners (participants/students) to hack. The innovation includes directions on how to set up multiple WiFi hacking scenarios that educators can implement in full or select as needed. The scenarios are (a) hacking WEP access points which have connected clients, (b) hacking WEP access points which have no connected clients, and (c) hacking WPA2 access points given a wordlist which includes the password educators should be looking for.

Educators will learn how Raspberry Pis can be used as the necessary clients for the WEP access points. Raspberry Pi scripts and all access point configuration directions are available online. Educators can also have access to a solution manual that describes how the different access points can be exploited.

BENEFITS

This innovation makes it feasible for educators to build an exploitable WiFi environment with a relatively low cost. The cost for the environment infrastructure is about $270, in addition to purchasing a WiFi USB adapter for each learner (which you can collect back after the learner completes their hands-on exercise) which costs about $25 a piece. The innovation and environment have been used in a higher-education setting and the preliminary results of the change in participant’s confidence (self-reported) to hacking WEP and WPA2 access points is significantly positive.

Once the environment is built, you can provide learners with a hands-on, evidence-based approach to understanding the difference between hacking scenarios where WEP access points have connected clients versus no connected clients in and the difference between hacking WEP vs WPA2 (given a wordlist).

CONTACT INFORMATION

Ahmed Ibrahim
a.i@virginia.edu
University of Virginia

DEVELOPING CYBERSECURITY WORK EXPERIENCE COMPETENCY MODEL

PRACTICE

DESCRIPTION

In collaboration with one of our industry partners; Forsyth Technical Community College has created a work experience opportunity for students. Students work and learn in our SOC Lab, monitoring networks for our affiliate organizations as our industry partners train them to utilize tools, navigate the ticketing systems, and analyze incoming and outgoing traffic. Students also utilize data analysis resources and hands on pen-testing equipment to specifically learn to recognize vulnerabilities and network threats. Students also learn the cyber threat hunting process as they begin their training as SOC technicians. Students will be trained on a weekly rotation during their 15-week CyberOps or Network Vulnerabilities class.

Our industry partners and stakeholders are confident that hands on training in a live SOC environment, cyber courses, reinforced competencies with threat hunting lab material, and verification of skills learned through industry training will equal student success, career success, and economic stability. The specific NICE work roles that these competencies align with are Cyber Defense Analysis and Cyber Defense Analyst, in the Protect and Defend Category/Specialty Area.

The SOC Lab will be one way to verify that the IT/Cyber and System Security curriculum being taught at Forsyth Tech, employing hands-on techniques and industry's learning strategies, are a sufficient baseline to validate student's competencies in Forsyth Tech cyber programs and also meet the needs of our industry partners.

BENEFITS

The SOC lab utilizes cyber threat hunting, which has emerged as a critical part of cybersecurity practice. Students are immersed in advanced analysis skills for cyber threat hunting. The Cyber Threat Hunting lab materials were sponsored by NSA, the University of North Carolina at Charlotte (UNC Charlotte) and Forsyth Technical Community College. These freely-available, hands-on teaching materials for cyber threat hunting are suitable for use in two-year community college curriculum, four-year universities curriculum, as well as for collegiate threat hunting competitions.

Forsyth Tech students will learn the following competencies (through practice in a live environment), which map to the NICE framework:

- Data analytics
- Communication
- Critical thinking
- Monitor networks
- Security analysis
- Vulnerability assessment
- Manage networks Analyze threats

CONTACT INFORMATION

Deanne Wesley

dwesley@forsythtech.edu

Forsyth Technical Community College

INTEGRATE STEPPING-STONE INTRUSION DETECTION INTO CYBERSECURITY CURRICULUM

PRACTICE

DESCRIPTION

Most intruders launch their attacks via stepping-stones. Detecting stepping-stone intrusions and preventing them from happening is significant. Most cybersecurity courses focus on teaching students' defensive techniques. Offensive techniques, such as Intrusion and its detection may be covered, but stepping-stone intrusion and its detection are rarely covered by most of the cybersecurity curriculum. In this innovation, I integrate stepping-stone intrusion detection and its prevention into two cybersecurity courses including Network security and Intrusion Detection and Prevention.

BENEFITS

The best way to defense is offense. Teaching students offensive techniques can help them to defend their computing system more securely and efficiently. Another benefit of this innovation is to arouse students' study interests on cybersecurity. Understanding attacking mechanism used by attackers can motivate our students to propose better ideas to secure computing systems.

CONTACT INFORMATION

Jianhua Yang

yang_jianhua@columbusstate.edu

Columbus State University

“HACKERS WANTED” TEDX TALK

PRACTICE

DESCRIPTION

This is a TEDx talk for students, educators and IT professionals on the need for more IT professionals using a Hacking motif. I also provide a three-step process for building cyber skills in students. In the fast-changing world of cybersecurity, the way to outmaneuver the adversary is to get inside their mind, outthink their strategy, and remain several steps ahead of them. This requires honing expert hacking skills, developing fast and agile responses, and strong creative problem-solving skills. It starts with reframing how we see hacking from a negative to a positive: to a tool to solve problems rather than a destructive force. Hackers Wanted...please apply now... your skills are needed to win the cybersecurity war.

BENEFITS

This brings the challenges of and solutions for building cyber professionals to a national stage.

CONTACT INFORMATION

Ronald Woerner
rwoerner@bellevue.edu
Bellevue University

K12-ISAC/ISAO/SOC

PRACTICE

DESCRIPTION

The mission of the K12-ISAC/ISAO/SOC is to build the maturity of cybersecurity risk management in the K-12 community by building and fostering a trusted community of K-12-focused security practitioners, curating and sharing cybersecurity information, promoting collaborative efforts, and creating and supporting efforts to strengthen faculty, staff, and students' cybersecurity knowledge and skills.

Along with creating a K12-ISAC/ISAO, another related goal is to create a K12-SOC, similar to OmniSOC (https://omnisoc.iu.edu), which is a new shared cybersecurity operations center for higher education. The K12-SOC would work in conjunction with the K12-ISAC/ISAO. Two benefits of a K12-SOC would be to provide SOC/CERT/CSIRT services to K-12 institutions that do not have the available resources to create their own SOC, and to educate students in a controlled environment to utilize necessary cybersecurity skills to meet the growing demand for cyber talent. One of the ideas for a K12-SOC would be to have portions of it be student manned. Students starting in 7th grade would begin learning cybersecurity through simulated SOC's and training tools. Students could begin working in the actual K12-SOC their 9th grade year, or sooner given the maturity level of the student. Part of the training would be for older students to mentor and train younger students (i.e. 10th mentors 9th, 11th mentors 10th, 12th mentors 11th, etc.). Older students would also help teachers provide education and awareness training to classrooms from K-12. Ideally there would be a partnership between local businesses and universities that would provide mentors and staff for the SOC. The SOC would also partner with companies that manufacture cybersecurity products that could be utilized by the SOC and provide real-world hands-on experience for the students.

One of the ideas we have discussed is students in the K12 program working with small business to help secure their environments. The idea would be that small businesses could approach the K12-ISAC/ISAO/SOC and request help. A team of students would then be assigned a project to work with the small business to help secure their environment. Students would be responsible, with guidance, for creating the project plan, performing initial risk assessments, developing security policies, user awareness training, etc. This would allow the students to gain experience in multiple areas and allow the business to have an inexpensive, maybe even free, security plan put in place.

Students would learn about leadership, proper business communication, doing the right thing, ethics, risk methodologies, privacy, how to talk with customers, project management, change management, budgeting, etc.; many things that get left out of traditional 'hacking' or red team programs. Security by design or DevSecOps would be a primary goal.

BENEFITS

Three primary needs that could be met with K12-ISAC/ISAO/SOC:

- Not enough resources to train teachers and administrators to understand cyber and teach cyber
- Not enough resources for K12 schools related to protecting infrastructure
- Not enough resources to train students for future cyber roles

CONTACT INFORMATION

Eric Lankford

eric.lankford@birdvilleschools.net

Birdville ISD/Global Resilience Federation

RUNCODE: PROVIDING REAL-WORLD PROGRAMMING CHALLENGES ACROSS ALL LEVELS OF DIFFICULTY FOR COMPETITORS FROM BEGINNING TO ADVANCED USING 16 DIFFERENT PROGRAMMING LANGUAGES

PRACTICE

DESCRIPTION

Learning to code takes time, motivation, and energy (for many it is something that we have to do on the side after hours from school or work). When someone starts to learn programming, they usually learn through either a programming class, bootcamp, or programming tutorial. However, once someone gains some programming knowledge, they struggle with finding ways to wield these new skills. The biggest barrier beyond those three articulated barriers is finding suitable problems or projects that require programming to solve. The RunCode platform is our attempt to fit within this gray area by providing over 180 language-independent coding challenges (with new ones being added periodically by the staff as well as player-donated challenges). On the RunCode platform, every time you solve a challenge, you earn points based on the difficulty of the problem. The top scoring players earn themselves a spot on the leader board. When you join the RunCode.ninja site you also get an invite to our Slack channel, our attempt to provide a community of support for all who want to work on RunCode challenges. In that Slack channel you have the opportunity to converse with like-minded individuals! The challenge authors all frequent the Slack channel and are available to answer questions about the site and about the challenges. All submissions are posted to the RunCode game channel in Slack so you can share your accomplishments (and trials) with the community. Succeed or fail, we're all in this together.

BENEFITS

The RunCode platform provides the following innovations: real-world programming challenges, code submission process, multiple supported languages, multiple test cases.

The RunCode platform provides individuals the opportunity to apply their freshly minted programming skills using real-world programming challenges. All of our challenges are written by cyber security practitioners or folks who wrote code for a living. When we develop challenges, we tend to lean on everyday challenges that we collectively have had to solve by writing some code. Oftentimes, we set up webpages, socket-based listeners, databases, or other supporting infrastructure to make our challenges more in line with real-world challenges.

The RunCode platform does not require the output of your code, it requires you to submit your code. We pull the code into a Docker container and execute/interpret the code against appropriate data sets, comparing the results against an expected answer. This process, and the use of Docker containers, allows us to create real-world programming challenges that can range from calculating some simple math and printing to standard output to interacting with sockets, webpages, filesystems, or even SQLite databases programmatically. We store every iteration of submitted code and provide the ability to download all of their submitted code for review. This allows them to review techniques used for solving particular problems and seeing how they have gotten better at solving programming problems over time.

Due to the unique way we assess competitor's submissions, we are able to receive solutions in a variety of languages. Currently, RunCode supports 16 different languages. This allows competitors to solve challenges in a language they are the most comfortable with or choose to start learning another language and solve or resolve challenges from the site.

RunCode reinforces local testing in conjunction with writing code. The localized testing requires individuals on the RunCode platform to look at the current programming challenge, the provided test case(s), and infer additional tests that may be required to solve the problem. This process scales with the challenge difficulty. With the easy challenges the site provides a very clear problem description and comprehensive test-cases. As the challenges become more difficult, the description becomes vaguer and the test cases may not address certain instances where we know the programmer may not write code that solves for all edge-cases. Additionally, since our solutions executes/interprets each competitor's code, we have absolute control over the test cases used. Again, for the easy problems the input data on the backend is the same as the test cases provided in the challenge descriptions. As the challenges become more difficult, we are able to add additional test cases that are not provided in the initial challenge description. This forces the competitor to conduct robust local testing.

CONTACT INFORMATION

Joshua Rykowski
jrykowski@augusta.edu
Augusta University

CYBER SECURITY TEAM TRYOUT

PRACTICE

DESCRIPTION

Students tryout for the UMGC Cyber Security Team using an open source CTF platform. Their coach set up a server running CTFd, created 10 categories that each have 10 questions. Students work on cybersecurity challenges in the categories of forensics, network forensics, malware analysis, password cracking and others. Students who score enough points are then added to the UMGC team's active roster. Students who do not score enough points, are given access to resources, such as Netlab, to improve their skills and are encouraged to tryout again at the next monthly tryout. A number of students have been able to join the team on the second or third try even after not having success during the initial tryout. Finally, there are active team members who monitor the discord channel to encourage students and help them go in the right direction, without providing answers to the puzzle questions. They give back because many of them were in a similar tryout situation and know that the words of encouragement can be extremely helpful.

BENEFITS

Many of the students are claiming that they are leaning more in the tryout than in some of their graduate or undergraduate courses (both graduate students and undergraduate students are allowed to tryout). Many students explain how they like being faced with a difficult challenge problem and working their way through it. The tryout exposes students to hands-on cybersecurity problem solving, which is a perfect complement to their traditional classroom experience. Students who earn their degree and also compete in competitions will have the ability to solve real-world high-level cybersecurity problems. Once they become a member of the team after successfully completing the tryout, they will be a member of an extended network of skilled cybersecurity individuals working together to learn more about their field. Members often seek out other members for job opportunities and internships. Active team members get a chance to compete in additional competitions which results in additional growth, knowledge levels, and employment opportunities. Students who get through the tryout successfully and become a member of the team are able to extend their network to other highly motivated like-minded people who want to take their cyber skills to the next level.

CONTACT INFORMATION

Jesse Varsalone
jvarsalone@gmail.com
University of Maryland Global Campus (UMGC)

04

PROGRAM DEVELOPMENT

WINNING SUBMISSION:
ACM CYBER2YR2020 CURRICULUM GUIDELINES

ACM CYBER2YR2020 CURRICULUM GUIDELINES

WINNER

PROGRAM DEVELOPMENT

DESCRIPTION

Offering guidance for a broad variety of cybersecurity programs at the post-secondary level, Cybersecurity Curricula 2017 (CSEC2017): Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity was the first effort at comprehensive cybersecurity curriculum guidelines. Using CSEC2017 as a starting point, the ACM Committee for Computing Education in Community Colleges (CCECC) has led creation of a similar set of guidelines for cybersecurity programs at the associate-degree level, called Cyber2yr2020 or Cyber2yr, formerly known as CSEC2Y. These guidelines specifically target two-year programs at community and technical colleges. Cyber2yr2020 focuses on curriculum guidelines for cybersecurity programs, including both transfer (A.S.) and career-oriented programs (A.A.S.) at the associate-degree level. The Cyber2yr2020 task force consisted of 10 members from community colleges across the United States, with an advisory group of individuals from industry, government, and four-year institutions. Two curriculum guide drafts were available for public commenting, and were presented in the United States as well as internationally in an attempt to gain as much feedback as possible to ensure a fully inclusive curriculum guide.

The curriculum guide focuses on student competencies. To ensure a breadth of knowledge, eight domains are included within the guidelines. These domains are data security, software security, component security, connection security, system security, human security, organizational security, and societal security. In addition to the eight domains, cross-cutting concepts are throughout the domains, including confidentiality, integrity, availability, risk, adversarial thinking, and systems thinking. Inclusion of these cross-cutting concepts will assist students in making connections between the domains and reinforce a security mindset conveyed throughout the cybersecurity curriculum. The competencies have been prepared with Bloom's Revised Taxonomy and align with national cybersecurity frameworks such as NICE, CAE, and ABET. Sample rubrics and program examples of use are also included within the Cyber2yr2020 curriculum guidelines.

BENEFITS

Benefits of using Cyber2yr2020 include:

- Conducting program reviews to update and create curriculum in cybersecurity. These guidelines can assist in the creation of both career and transfer curriculum, as well as certificate credentials
- Facilitating programs and course articulation. Two-year cybersecurity programs can use these guidelines to establish conversations with four-year institutions that have similar cybersecurity programs. Since the cybersecurity competencies and learning outcomes were used by ABET to develop criteria for two-year cybersecurity programs, two-year and four-year institutions can benefit from program-specific criteria provided in this document
- Complying with government-sponsored frameworks: The ACM CCECC cybersecurity competencies align to the NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, as well as to the Centers of Academic Excellence - 2019 Foundational Core and Technical Core Knowledge Units
- Interacting with local advisory boards: The guidelines' competencies provide a framework for discussion of cybersecurity competencies, courses, certificates, and degrees, permitting a program's advisory board to review competencies and learning outcomes with local needs in mind

CONTACT INFORMATION

Cara Tang

cara.tang@pcc.edu

ACM Committee for Computing Education in Community Colleges

CYBERTECH GIRLS: DEVELOPING INTEREST IN CYBERSECURITY EDUCATION AND CAREER PATHWAYS

HONORABLE MENTION

PROGRAM DEVELOPMENT

DESCRIPTION

Cybersecurity professionals are often required to think like an adversary, to implement security strategies that defend systems against the unexpected. Building an inclusive cybersecurity workforce requires diverse groups of people with skills that can be leveraged to build secure systems, to raise public awareness about cybersecurity, and to mentor others on the pathway to cybersecurity careers. Today's cybersecurity workforce is unbalanced due to the underrepresentation of women and minorities in the field. In order for tomorrow's cybersecurity workforce to be diverse and inclusive, leaders in academia, government, and industry should focus on developing student pathways that lead to education and career in cybersecurity.

First offered at Coastline College in 2016, CyberTech Girls is a one-day cybersecurity pathway event for middle school and high school girls. The founder of CyberTech Girls has also assisted others with their events offered at other community colleges and universities across the southwestern region, including California, Colorado, and Nevada. Attendance at each event has ranged from 50-125 middle school and high school girls. The program aims to introduce cybersecurity concepts to develop youth interest in cybersecurity education and careers. CyberTech Girls events include hands-on activities and workshops to introduce cybersecurity concepts, share information about cybersecurity education pathways and careers, empower youth girls and help them feel inspired to empower others, and help the youth girls find ways to continuously engage in cybersecurity activities post-event.

As part of the pathway, the CyberTech Girls program introduces the CyberPatriot competition, how to start a student cybersecurity club, local dual-enrollment and higher education offerings, and professional organizations. Female mentors working in cybersecurity and technology roles share their experiences and education that led to their current roles. The CyberTech Girls agenda intends to keep the girls continuously engaged in hands-on activities, with rotating workshops including digital forensics with evidence collection in a mock crime scene followed by forensic analysis in the lab, computer desktop assembly, website design featuring cybersecurity topics, and capture-the-flag competition.

BENEFITS

CyberTech Girls events focus on hands-on activities that engage attendees with the concepts of cybersecurity to build an ongoing interest. Female mentors share their stories and help to run the workshop activities to provide youth girls with a fun cybersecurity experience that builds lasting memories. The hands-on events bring together a wide range of females interested in cybersecurity: youth girls in middle school and high school, college students, professional mentors working in industry, government, and academia. CyberTech Girls brings the community together to further develop pathways and continue developing youth interest in cybersecurity.

CONTACT INFORMATION

Tobi West
twest20@coastline.edu
Coastline College

MOBILE PHONE PHYSICAL ACQUISITION TRAINING IN NETLABS

PROGRAM DEVELOPMENT

DESCRIPTION

We conducted a summer case study on mobile forensics and were able to figure out a way to allow students to accomplish actual physical vs logical acquisitions of mobile device equipment from with the NDG Netlab platform. To our knowledge, this has not been done before. On a scale of 1 to 10 for training importance in physical device acquisition vs logical device acquisition, the physical ranks at an 8 and the logical is only around a 3 or 4, according to our SMEs that assisted us with objective and methods development.

BENEFITS

Students can perform physical device acquisition in a virtual environment. Therefore, we are able to keep possession of the devices to ensure longer life. Also, the students can perform the acquisitions virtually from anywhere that they have Internet access. We do not have to provide mobile devices that may not return, which would dwindle our inventory in an accelerated way. A physical acquisition is the only way we've been able to obtain deleted data that students can also gain experience recovering and looking for.

CONTACT INFORMATION

Tonya Davis
tonya.davis@tridenttech.edu
Trident Technical College

SOCALCCCC - SOUTHERN CALIFORNIA CYBERSECURITY COMMUNITY COLLEGE CONSORTIUM

PROGRAM DEVELOPMENT

DESCRIPTION

Developing cybersecurity education pathways for youth and adults interested in re-skilling to prepare for new careers is a passion of SoCalCCCC. Comprised of faculty, administrators, and program coordinators of higher education in Southern CA, this diverse group provides leadership and mentorship for students and professionals interested in cybersecurity. Originally formed in 2015 by faculty from Coastline College, Cypress College, Irvine Valley College, and Long Beach City College, SoCalCCCC monthly meetings include others from the region: Fullerton College, Rio Hondo College, and Webster University. SoCalCCCC develops pathways to engage students in hands-on activities to build skills for the cybersecurity workforce of tomorrow.

SoCalCCCC notable efforts:

- Coastline offers monthly CyberPatriot training to 100+ students in 2015, followed by similar programs at Cypress, Irvine Valley, and Long Beach CC
- As SoCalCCCC, Coastline, Cypress, and Irvine Valley College designated a CyberPatriot Center of Excellence in 2016
- Coastline hosts annual CyberTech Girls for 50-125 youth girls and assists colleges in the southwestern region with similar events
- A founding member of SoCalCCCC moved to Cabrillo College to continue significant efforts with cybersecurity competition in Northern CA
- Coastline hosts annual CyberTech Expo, raising community awareness about cybersecurity
- Coastline started CA Cybersecurity Apprenticeship Program, offering online cybersecurity courses and on-the-job training for qualified apprentices
- Coastline designated Southwestern CAE Regional Resource Center by NSA
- Coastline faculty partnered with Fullerton College on Cyber Up! to develop an A.S. degree in Digital Forensics & Incident Response for Coastline - NSF #1800999
- Coastline formed the Southern CA Netlab Regional Center, hosting remote labs for 30+ colleges and high schools
- Fullerton College hosted 100 girls from the Girls Scouts of OC to earn cybersecurity badges in 2018
- Coastline re-designated as a Center of Academic Excellence in Cyber Defense Education in 2019
- Webster University hosts monthly ISACA presentations
- Coastline hosts the Western Regional Collegiate Cyber Defense Competition
- Cypress, Long Beach, & Webster University designated CAE in 2019
- Coastline partnered with faculty from Irvine Valley College to host GenCyber Girls, a summer camp with female mentors from industry, FBI, NSA, and Cal Poly Pomona
- Cypress's PACE project receives NSF award #1902519 to develop cybersecurity education pathways
- Coastline's Cybersecurity program receives ASCCC 2020 Exemplary Program Award

BENEFITS

Each college of SoCalCCCC serves as a model for its premiere program to help others in the region develop similar programs or cross-promote unique programs like CyberTech Girls at Coastline. Together, the members of SoCalCCCC have built the second largest CyberPatriot Center of Excellence in the nation and partnered on NSF-funded activities, such as Cyber Up! and GenCyber Girls at Coastline, to bring together high school teachers and college faculty.

SoCalCCCC efforts have established an inviting and collaborative group of community college and university members that build education and competition pathways to develop the future cybersecurity workforce. Founding members have continued to share their passion for cybersecurity throughout the state, including the start of a new cyber competition called Purple Competition hosted by Cabrillo College and San Francisco City College. Over the past five years, thousands of K-12 and college students have participated in the cybersecurity outreach pathways established by SoCalCCCC.

CONTACT INFORMATION

Tobi West
twest20@coastline.edu
Coastline College

HOW TO EARN A CYBERSECURITY ASSOCIATES AND BACHELORS DEGREE TWO YEARS AFTER HIGH SCHOOL COMPLETION AND FOR LESS THAN $15,400, INCLUSIVE OF ALL RESOURCES AND CERTIFICATIONS

PROGRAM DEVELOPMENT

DESCRIPTION

Cincinnati State and WGU Ohio have developed a transfer pathway that allows high school students to use College Credit Plus (CCP) credits to earn their Associates degree, A.A.S. Computer Networking Engineering Technology - Cyber Security Major by year 12 of high school. The student then enrolls into WGU Ohio's online, competency-based program, transferring in 61 credits toward a B.S. in Cybersecurity and information Assurance. They can then earn their B.S. degree in two years or less for less than $15,400, inclusive of resources and certifications.

BENEFITS

Students earn their associates degree with no out of pocket expense, and during their years in high school. Students earn their bachelor's degree in two years or less, post high school, for a fraction of the cost of a State school in Ohio. This saves the student both time and money. The student is ready for an in-demand career two years earlier and has little to no debt from their college education.

CONTACT INFORMATION

Krista Spencer, Paul Weingartner

krista.spencer@wgu.edu / paul.weingartner@cincinnatistate.edu

Cincinnati State and Western Governors University (WGU), Ohio

WGU’S NEW IT MICROBACHELORS PROGRAM LETS STUDENTS EARN WORK-READY CREDENTIALS ALONG THE PATH TO A DEGREE

PROGRAM DEVELOPMENT

DESCRIPTION

Western Governors University (WGU) announced the university’s first globally available microcredential in Information Technology (IT). WGU’s IT Career Framework MicroBachelors is designed to create pathways for individuals looking to advance their IT careers. Credit-backed and stackable, WGU’s new microcredential provides value as a standalone credential, but also allows busy working learners to apply credit towards a bachelor’s degree program at WGU, pending admission.

According to the U.S. Bureau of Labor Statistics, employment in computer and IT occupations is expected to grow 12 percent from 2018 to 2028, much faster than the average for all occupations. And according to CompTIA’s 2019 Cyberstates Report, there were 3.7 million postings for tech occupation job openings in 2018 alone. By partnering with IT industry leaders, WGU has designed this new stackable credential to give learners the foundational skills they need to compete for high-growth, lucrative computer science and IT careers, helping close the IT skills gap.

WGU’s IT Career Framework MicroBachelors provides learners with the in-demand computer networking, security, scripting, and programming skills they need to compete in a dynamic, tech-driven economy. Developed to provide learners with incremental value at the course level, WGU’s new microcredential is perfect for adults who want to add skills to their profiles but may not necessarily pursue a bachelor’s degree. For learners who are interested in pursuing a bachelor’s degree, the new microcredential stacks into seven different IT bachelor’s degree programs at WGU: B.S. Computer Science, B.S. Software Development, B.S. Cloud and Systems Administration, B.S. Data Management/Data Analytics, B.S. Information Technology, B.S. Cybersecurity and Information Assurance, and B.S. Network Operations and Security.

Like all WGU degree programs, the IT Career Framework MicroBachelors is competency-based, allowing students to advance as soon as they demonstrate mastery of course materials. WGU’s new program can be completed for less than $1,500, making it possible for busy learners to advance their careers without breaking the bank. Like all edX courses, learners can choose to access course materials for free but will only be granted credit through successful completion of the verified MicroBachelors certificate.

BENEFITS

WGU’s IT Career Framework MicroBachelors provides learners with the in-demand computer networking, security, scripting, and programming skills they need to compete in a dynamic, tech-driven economy. Developed to provide learners with incremental value at the course level, WGU’s new microcredential is perfect for adults who want to add skills to their profiles but may not necessarily pursue a bachelor’s degree. For learners who are interested in pursuing a bachelor’s degree, the new microcredential stacks into seven different IT bachelor’s degree programs at WGU: B.S. Computer Science, B.S. Software Development, B.S. Cloud and Systems Administration, B.S. Data Management/Data Analytics, B.S. Information Technology, B.S. Cybersecurity and Information Assurance, and B.S. Network Operations and Security.

CONTACT INFORMATION

Krista Spencer

krista.spencer@wgu.edu

Western Governors University (**WGU**)

IQ4 VIRTUAL INTERNSHIPS IN CYBER SECURITY (STUDENTS PREPARE FOR CYBER SECURITY JOBS)

PROGRAM DEVELOPMENT

DESCRIPTION

For the past five semesters, the Saint Peter's University Department of Computer & Information Sciences has worked with iQ4 Corporation to team-up to offer two virtual internships that span an entire semester. The internships have been incorporated in the University catalog, average 18 students, and are becoming increasingly popular on campus. The virtual internships offered are:

- Insiders Threat - An Epic Challenge (students work on projects associated with the NIST Cybersecurity Framework relating to the identification, detection, protection, response, and recovery from a cyber-attack)
- Cyber Crimes - Web's Dark Side (students work on projects associated with cybercrime: fraud, theft, assault, terrorism, extortion/ espionage, and trafficking)

For both virtual internships, students become "cyber interns" and work in teams with faculty and industry experts as mentors using the iQ4 online/cloud communication platform. The goals of the internships are to enable students to analyze real cybersecurity case scenarios and identify the depth and breadth of cybersecurity from multiple perspectives. Students focus on the interrelated dimensions of cyber threats (which may include but are not limited to technical, procedural, legal, behavioral, skills/proficiencies) and the spectrum of constituent cyber domains/functional areas in which to identify solutions. The content for the internships covers student core competencies (e.g., knowledge, skills, and abilities) including how to build and maintain communications with executives, peers and regulators. Essential skills (e.g., teamwork, critical thinking, and communications skills), which are required in the workforce are also acquired. The assignments/projects in the virtual internships are designed to assess both core competencies and essential (soft/professional) skills.

As a Professor at Saint Peter's University, I find the experience the students are getting very valuable, providing them with cybersecurity as well as soft skills (e.g., public speaking, defending your point of view) while always keeping an eye on the job market. iQ4 accomplishes this by bringing real employer experience into the classroom and providing a holistic workforce development platform.

The iQ4 virtual internships provide a robust combination of cutting-edge applied learning technology, standards-based taxonomies, and industry expertise brought into the classroom that had added great value to our students and we look forward to continuing and building further our partnership with iQ4.

BENEFITS

- Industry-driven curricula on the iQ4 workforce development platform, easy to plug and play, and fits seamlessly into the academic curriculum
- Case studies created by industry subject matter experts
- Students receive a Digital Skills passport, a multimedia resume. They can select job roles that use the NICE SP 800-181 skills taxonomy within projects
- Weekly mentoring sessions with seasoned professionals who provide real-world knowledge

- Development of collaboration, writing, presentation, analysis, and communication skills
- Customized curricula delivered either virtually or in a hybrid model of virtual and classroom format
- Internships focus on the student experience, engagement, and learning outcomes
- Experiential education that builds career pathways.

CONTACT INFORMATION

Suman Kalia
skalia1@saintpeters.edu
Saint Peter’s University

TECH-IN-RESIDENCE CYBER CORPS

PROGRAM DEVELOPMENT

DESCRIPTION

The NYC Tech Talent Pipeline launched the Tech-in-Residence Corps in 2017: The Corps is made up of industry professionals who teach courses in tech majors across New York City to bring students the in-demand skills and project experience they need to launch careers in tech. The Tech-in-Residence Cyber Corps was launched in 2019 as part of Cyber NYC: A multi-pronged New York City Economic Development Corporation (NYCEDC) initiative dedicated to making NYC a global leader in cybersecurity.

As part of the Applied Learning arm of Cyber NYC, the Cyber Corps recruits information security professionals and provides them with the training necessary to share their experience and knowledge with students across the city. In their roles as adjunct professors, Cyber Corps candidates work with faculty mentors to teach upper level undergraduate courses and contribute to the design of industry-informed curriculum within Computer Science, Computer Engineering, and Computer Information Systems departments. The Corps is comprised of candidates with expertise in various domains of security, and the courses created through these partnerships reflect this diversity; sample courses include: Secure Software Engineering, Cyber Risk Management, Cybersecurity and Digital Operations, Web Security, and more. Syllabi for these courses are made publicly available and can be found at OER Commons.

New York City cybersecurity professionals interested in teaching with the Cyber Corps are encouraged to submit an application.

BENEFITS

- Students in Tech-in-Residence Cyber Corps classes supplement their academic coursework with lessons and hands-on projects that reflect trends in industry, which prepare them for in-demand cybersecurity careers
- Students in Cyber Corps classes are able to network with and learn from cybersecurity analysts, engineers, and executives at leading companies, connecting them with opportunities to pursue internships, apprenticeships, and entry level security careers
- Curriculum developed as a result of Cyber Corps partnerships leads to the development of industry-informed courses. The syllabi for Cyber Corps courses are publicly available for educators looking to teach cybersecurity

CONTACT INFORMATION

Gotham Sharma
gsharma@sbs.nyc.gov
NYC Tech Talent Pipeline

75% SCHOLARSHIP FOR U.S. RESIDENTS

PROGRAM DEVELOPMENT

DESCRIPTION

NYU Tandon School of Engineering launched the NYU Cyber Fellows, which provides a 75% scholarship towards tuition for our elite online Cybersecurity Master's Degree. Thanks to generous support, this first of its kind program will be offered for the affordable price of approximately $16,000 and will include access to a hands-on virtual lab, industry collaborations, industry-reviewed curriculum, exclusive speaker events, and peer mentors.

BENEFITS

The scholarship increases the size of participation in the cyber security workforce by US Residents.

CONTACT INFORMATION

Aspen Olmsted
ao56@nyu.edu
New York University

COMMUNITY-BASED LEARNING IN CYBERSECURITY & CYBER FORENSICS

PROGRAM DEVELOPMENT

DESCRIPTION

Community-based learning is a teaching and learning strategy that integrates meaningful community engagement with instruction and reflection to enrich the learning experience with a greater emphasis on reciprocal learning and reflection. Community Based Learning (CBL) is a pedagogical approach that is based on the premise that the most profound learning often comes from experience that is supported by guidance, context-providing, foundational knowledge, and intellectual analysis. The opportunity for students to bring thoughtful knowledge and ideas based on personal observation and social interaction to a course's themes and scholarly arguments brings depth to the learning experience for individuals and to the content of the course. The communities of which we are a part can benefit from the resources of our faculty and students, while the courses can be educationally transformative in powerful ways.

BENEFITS

A key element in applying the community-based learning approach to cybersecurity & cyber forensics is the opportunity students must both apply what they are learning in real-world settings and reflect in a classroom setting on their service experiences. Examples include: mentorship of college students to high school students in cybersecurity competitions such as AFA's CyberPatriot, National Cyber League (NCL), and serving as student mentors and assistants in NSF/NSA's GenCyber camp. These programs model the idea that giving something back to the community is an important college outcome, and that working with community partners is good preparation for citizenship, work, and life" (Association of American Colleges & Universities | https://www.aacu.org/leap/hips). The ability to offer college credit for such experience(s) is an incentive for students to pursue community-based learning opportunities.

CONTACT INFORMATION

Josh Brunty
josh.brunty@marshall.edu
Marshall University

NEARLY DOUBLING NUMBER OF FEMALE AND MALE STUDENTS IN CYBERSECURITY PROGRAM IN FIVE MONTHS

PROGRAM DEVELOPMENT

DESCRIPTION

Nearly Doubling Number of Female and Male Students in Cybersecurity Program in Five Months

Description of Innovation: After participating in a WomenTech Educators Onsite Training, Fayetteville Technical Community College (FTCC) increased female enrollment in the introductory courses in the Cybersecurity A.S. Program by 12 female students - from 12 to 22 women in five months. Male enrollment also increased from 58 to 101.

FTCC hosted a WomenTech Training conducted by Donna Milgram, Executive Director of the National Institute for Women in Trades, Technology & Science, in March 2019. Four teams participated from four career pathways, one of which was Cybersecurity. In five months, the Cybersecurity team nearly doubled the number of female and male students and exceeded their recruitment goal.

A team of 12 key stakeholders in Cybersecurity education - including the Chair of the Networking Department and six instructors - developed a robust WomenTech Recruitment Plan using the plan template provided in the WomenTech Training.

One of FTCC's key strategies was to repurpose a "Monthly Tech Talk" event at the college and turn it into a recruitment event. It became a "Women in Technology Tech Talk" and the messaging was, "It's Ladies' Day at FTCC Computer Technology/Cybersecurity Labs!" Publicity included "Men are welcome too!" and indeed some came.

Female role models in cybersecurity were featured during the two-hour event. The keynote speaker was in the military reserve and a consultant for Booz Allen Hamilton. The women spoke about their experiences, career pathways and encouraged participants to register for the introductory courses. Interviews with the Cybersecurity Chair and footage of the Tech Talk are included in this short video developed by FTCC: https://youtu.be/8hMD-lR1SLg.

BENEFITS

Nearly doubling the number of female and male students in Cybersecurity Education in a field with an extreme labor shortage of women and men. Retention of female students because of curriculum changes that increase engagement.

CONTACT INFORMATION

Donna Milgram
donna_milgram@iwitts.org
National Institute for Women in Trades, Technology & Science

PH.D. PROGRAM COMPLETION PLAN IN CYBERSECURITY EDUCATION

PROGRAM DEVELOPMENT

DESCRIPTION

NDSU launched a degree completion plan within our Ph.D. in Computer Science focused on cybersecurity education. We've already started our first four-student cohort in this program. Students pursuing this degree completion plan focus their dissertation and course selections on cybersecurity education, in addition to meeting all of the normal course requirements for the NDSU Ph.D. in Computer Science. The goal of this program is to prepare individuals who want to be college/university level faculty teaching in the area of cybersecurity. It gives them the skills and tools needed to design best-of-breed cybersecurity curriculum and assess it.

BENEFITS

The Cybersecurity Education Ph.D. Completion Plan provides an opportunity to specialize in cybersecurity education. We believe that this is a first-in-the-nation program which is directly responsive to a key area of national need (i.e., for college/university faculty to teach in the area of cybersecurity). Students in this program learn the basics of computer science through our required sequence. They also learn about key areas in cybersecurity (e.g., research methods, defensive security, ethical hacking, forensics and policy). This graduate-level technical content ensures that they are prepared to offer high quality technical instruction and further develop their skills to teach about the new technologies, attacks and security paradigms of tomorrow. Students then focus their remaining coursework, research and dissertation on cybersecurity education and its assessment. This results in research on new techniques of cybersecurity instruction and their assessment. When done, the program graduate is well prepared for both key aspects of being a cybersecurity faculty member: research and teaching within the discipline.

CONTACT INFORMATION

Jeremy Straub
jeremy.straub@ndsu.edu
North Dakota State University

NSF

NATIONAL
CYBERWATCH
CENTER

WWW.NATIONALCYBERWATCH.ORG
WWW.NATIONALCYBERWATCH.ORG/INNOVATIONS