NATIONAL CYBERWATCH CENTER

2018 INNOVATIONS IN CYBERSECURITY EDUCATION

Table of Contents

01. CURRICULUM

02. FACULTY DEVELOPMENT

03. LAB ACTIVITY

Table of Contents

04. LOCAL PARTNERSHIP

05. STUDENT LEARNING AID

Message from the Director

The National CyberWatch Center continues to build on its robust collaboration platform to support an informed community of interest in cybersecurity education and workforce development. A symbol of this commitment is the second annual Innovations in Cybersecurity Education program.

This year for the first time, select submissions will be eligible for inclusion in our newly launched *Cybersecurity Skills Journal: Practice and Research (CSJ)*: **csj.nationalcyberwatch.org**.

Moving forward, we will be exploring the growth of the Innovations program in areas such as: career promotion, performance models and measurement (theory/assessment), effective practices (techniques, tactics, procedures), capability maturity development (instruction), and the exchange of innovations across our members.

Thanks to all who submitted proposals this year and a special congratulations to the five winners!

Sincerely,

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

National CyberWatch Center Not a Member Yet?

The Innovations in Cybersecurity Education program highlighted here is one of many capacity building efforts undertaken by the National CyberWatch Center to strengthen the quality and quantity of the cybersecurity work force of our nation. In order to enhance our ability to serve the diverse audience that depends on our services, we have begun to implement a membership model that reaches out to the academic community and beyond to establish a network of activists who can help push our aggressive agenda forward.

Before the new academic year begins, now is the best time to secure your membership in the Center. This powerful, 700+ person network of cybersecurity professionals and educators is supported by a member management system that can ultimately help you:

- **Advertise** (e.g., job or faculty openings, new programs, or events)
- **Ask for** leads and opinions on resources (e.g., labs, textbooks, articles)
- **Solicit** collaborators for your new ventures
- **Receive** information on new grant opportunities, distributed only to members
- **Participate** in curriculum research, sponsored by the National CyberWatch Center
- **Access** links to new publications prior to public release
- **Qualify for discounts on registrations** for National CyberWatch-sponsored events such as the MACCDC.

Whether you're a faculty member at an academic institution, a career professional, or a corporation that would like to be affiliated with the National CyberWatch Center, you can increase your "reach" and take advantage of this powerful professional network just by becoming a member. Documents on each of the member plans are available at: **https://nationalcyberwatchcenter.wildapricot.org/join-us**.

01

CURRICULUM

WINNING SUBMISSION:
COMMUNITY INITIATIVE CENTER OF EXCELLENCE FOR SECURE SOFTWARE (CICESS) - EMPLOYER-LED SECURE SOFTWARE DEVELOPMENT DUAL MODEL APPRENTICESHIP PARTNERING WITH COMMUNITY COLLEGES

COMMUNITY INITIATIVE CENTER OF EXCELLENCE FOR SECURE SOFTWARE (CICESS) - EMPLOYER-LED SECURE SOFTWARE DEVELOPMENT DUAL MODEL APPRENTICESHIP PARTNERING WITH COMMUNITY COLLEGES

CURRICULUM

DESCRIPTION

An employer-led unique industry/government/academic collaboration of Central Illinois employers partnering with Illinois Central College (ICC) and supported by the National Initiative for Cybersecurity Education (NICE), Department of Labor Office of Apprenticeship and the Department of Homeland Security resulted in the creation of a first-inthe-nation two-year AAS degree program in Secure Software Development. The collaborative effort demonstrated how community colleges working with industry can create pathways to indemand high wage, high technology jobs through a dual model apprenticeship. The collaborative effort's innovation pioneered the degree program which incorporated the Carnegie Mellon University Software Engineering Institute's (CMU/SEI's)software assurance curriculum recommendations at the community college level and is aligned with the NICE Cybersecurity Workforce Framework. Timeline: In October 2013, in response to the rise in 31 cyberattacks and the need for secure software development, three employers in Peoria, Illinois– Ishpi Information Technologies, CEFCU, and Illinois Mutual - formed an ad hoc group to promote dual model apprenticeships to create a talent pipeline of software developers trained, mentored, and certified to develop software which is secure from cyberattacks. Dual here means that, in addition to technical instruction in a vocational school/college, the apprentices receive relevant practical training and mentoring at a partnering company, while receiving a salary as they gain work-related skills. There is a growing awareness that the U.S. could reap substantial benefits from dual model apprenticeships. The employer group decided to partner with ICC, the local community college to provide the related technical instruction in the dual model apprenticeship. The group received valuable input from the (NICE) Workforce Framework, the Department of Labor Office of Apprenticeship, the Department of Homeland Security and CMU/SEI. The group established several lofty goals for the dual model apprenticeship initiative which they named the Central Illinois Center of Excellence for Secure Software (CICESS).

BENEFITS

The CICESS initiative has created the following artifacts which are available in the public domain at no cost:

1. Standard secure software development curriculum that meets CMU/SEI guidelines for software assurance education in community colleges
2. Standard on the job training curriculum topics and secure software development competencies
3. Occupational standard, work process schedule, and validation of competencies in a DoL Registered Apprenticeship Standard for Computer Programmer (Secure Software)

CONTACT INFORMATION

Girish Seshagiri
girish.seshagiri@ishpi.net
(703) 426-2790
Illinois Central College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

A VISUAL PRIVACY THEMED EDUCATIONAL MODULE USING SOCIAL MEDIA APPS FOR PRIVACY AWARENESS AND CYBERSECURITY OUTREACH

CURRICULUM

DESCRIPTION

With the advent of internet (World Wide Web) and social media, and the extensive use of these resources by users with no technical backgrounds (naïve users), including K-12 youth, privacy issues come up every now and then. The lack of awareness about cyber-security, especially privacy related aspects, during the use of online web contents and social media, leads to avenues by which confidential information can be leaked and the user's privacy can be compromised. The current IEEE/ACM computing curriculum clearly points to a need for inclusion of societal privacy topics within the present body of knowledge areas so that a general awareness can be created regarding today's growing privacy concerns, including that with media sharing and public surveillance. There has been some computing educational research with curriculum development on the topic of data privacy. However, there has been very few efforts towards designing a pre-university outreach curriculum on visual privacy, with focus on the privacy-enhanced computer vision theme, especially at the K-12 level, using a social media platform. Our innovative hands-on learning activity intends to address the requirement of establishing privacy awareness in the community for the use of social media. It is motivated by the need of a visual privacy curriculum at the K-12 level. Its main contribution is the design and development of a creative outreach workshop for privacy education using social media apps. It presents a unique visual medium-based hands-on workshop that employs the PVA (Privacy through Visual Anonymity) theme to teach privacy notions using images and videos via social media apps. Our innovative PVA educational module involves two freely accessible social media applications, namely an android mobile app (Obscura Cam) and YouTube (YouTube-FaceBlur utility). These social media apps are utilized to illustrate the concept of visual privacy and visually demonstrate privacy preservation through the mechanism of visual anonymity in online pictures and video clips. Our PVA workshop module has been hosted with different middle-school audiences as part of a summer STEM academy and a Google Ignite CS program respectively.

BENEFITS

Our innovative educational module on visual privacy using social media apps has the following benefits:

1. Creation of privacy awareness and generation of interests in cybersecurity topics among youth
2. Potential workshop module for privacy education, outreach and recruitment at the K-12 level
3. Simple yet effective tool for privacy literacy in regard to social media and visual content (as it can help build privacy perceptions in the young minds and contribute to community awareness)

CONTACT INFORMATION

Muath Obaidat
Ankur Chattopadhyay
chattopa@uwgb.edu
(920) 465-5679
University of Wisconsin - Green Bay (UWGB)

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

BUSINESS SAVVY CYBERSECURITY

CURRICULUM

DESCRIPTION

We designed a lab environment that contains six different mini businesses with the help of a Cybersecurity Workforce Education grant from NSA. The classroom is divided into six individual business pods that function as if they were a business from one of six sectors. The sectors we concentrated on initially were finance, education, transportation, manufacturing, government and healthcare. Students are assigned to businesses as freshman and each student has a different job selected from NIST job descriptions. Students are introduced to their particular business as freshman in the computer support class where they need to write resumes, job descriptions and interview. After they are "hired" they are introduced to their new business with no directions. They are told that they just got hired and they need to complete the duties of the job they were hired for.

Each student business has a wireless access point, switch, firewall and two desktop computers. The businesses all run their own mini networks, but can communicate with the other mini business networks. Student businesses have databases and websites typical of their business. The students need to research to decide which rules/regulations/policies their business must follow. They need to write and implement policies for their business. After student teams have had a chance to get comfortable with their business, a student "red team" will attack all of the businesses. Red teams will also be responsible for doing penetration testing reports for businesses after the first round of attacks. The entire mini business lab has been setup and run by students.

BENEFITS

Students that use their skills to "work" in a real world setting are better prepared to enter the workforce. Many times they learn the tools of cybersecurity, but are unsure which situation they should use them in. Working in a business environment, students get a holistic view of cybersecurity. They are able to use upper level skills such as design, creation and analysis in a situation where they can actually see the results of their work. This setting is highly motivational to students. Students have only started to use this lab in the past month. However, in their first day of really working in the lab, none of the students left at the end of class. In fact, some of them stayed until the college was almost closing.

CONTACT INFORMATION

Vickie McLain
v.mclain@lsc.edu
(218) 733-7763
Lake Superior College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

CASE STUDY: MATERIAL WEAKNESS AS A RESULT OF A CYEBRSECURITY INCIDENT

CURRICULUM

DESCRIPTION

In mid-2017 a major US-based publicly traded corporation announced to the SEC that, as a result of a cybersecurity incident, they were reporting material weaknesses that could impact both their financial and operational results. In the first two quarters since that time, remediation costs totaling about $400M have been written off by this corporation. This teaching case introduces the background and the cyber incident impacting this organization.

BENEFITS

This case has been used quite successfully with almost 200 MBA students, introducing topics such as cybersecurity principles, cyber considerations in goverance and merger/acquisition activities, enterprise risk management, crisis communications and incident response and the aftermath of a cyber incident. Students gave strong feedback on the case because it was timely, allowed them to approach these hard to grasp cyber principles from a business perspective, and emphasized the need to consider the impact of cybersecurity preparation, planning and response.

CONTACT INFORMATION

Bill Hefley
Bill.Hefley@utdallas.edu
(972) 883-5006
The University of Texas at Dallas

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

CHOOSE YOUR OWN ASSESSMENT

CURRICULUM

DESCRIPTION

One of the difficulties when assessing student understanding is to ensure the areas a student has learned (as well as those they have not) are assessed. It can also be difficult for students when learning a subject in cybersecurity to write a paper about it instead of applying what they learned or pushing beyond what is offered in the classroom, such as if the student develops a real interest in the topic and is inspired to delve deeper via personal research and application. As an educator it can be very boring to read about the same topic, which essentially comprises of a restatement of historical facts on the item, especially when that information is already known. In Andragogy (the teaching of adults) we serve them best when we offer an opportunity for immersion, offer context, provide learning materials in support of multiple learning styles, and inspire creativity and innovation. For many years I have offered the final project (whenever permissible, having taught for many schools) as 'Choose your own Assessment' wherein students decide how they show and convince me of what they learned. I have crafted a number of rubrics (which I can share) to address papers, projects, presentations, new tool creation, etc. All projects include a final presentation (in person if an on- ground class, live via webinar or recorded depending on the online platform and location of the student where the student shares their creation along with some of the project management they undertook and the process by which they developed their project. This has resulted in some wonderful projects including repeatable templates for policies, web design templates in a variety of languages and tools, pentest reports of real businesses that have contracted the student, risk assessments performed on businesses, a student's own distribution of Linux (not simply adding tools to Ubuntu or another flavor, but building from the ground up with a kernel, shell, boot loader, package manager, desktop manager, tools, etc and the enhancements to pull the wireless data from the wind turbines on campus and allow for statistical processing and graphing of that data to determine uptime, required maintenance, most productive hours, days, weeks, etc).

BENEFITS

The student is empowered to learn more about whatever facet of the subject area interests them. The requirements state the student must move beyond what is covered in class and present something that we would not learn if not for their project. Students conduct research, manage a project including several deliverables and milestones, they must effectively communicate their project results and include effective communication relative to their project (such as in the Linux distro there was documentation created for the user, for policy templates there was how-to instructions created, public speaking is required in the presentation of their ideas, and as adults they get to make choices about their learning and the application thereof. This has led to increased satisfaction in many classes - especially those that traditionally resulted in a large paper on the dry subject matter. Students are also seen as subject matter experts by their peers. I have watched this continue into subsequent classes as often the student continues to pursue the topic or similar topics throughout their academic career.

CONTACT INFORMATION

Denise Kinsey
denisekinseytx@gmail.com
419) 470-9095
University of Houston

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

CREATE A CYBER INTERNSHIP PROGRAM WITHIN AN ACADEMIC ENVIRONMENT

CURRICULUM

DESCRIPTION

An essential outcome of all cybersecurity curricula must be that graduates are prepared to apply the knowledge they have obtained to the practice of cybersecurity. To support this outcome, Anne Arundel Community College (AACC) implemented an internship structure to give students a deeper experience using cybersecurity tools. The focus of this internship is to investigate and use a cybersecurity tool and develop a hands-on scenario/lab for the tool. Interns are paired with a cybersecurity faculty member who guides them through the investigation and use of the tool, development and delivery of the scenario/lab, and documentation of the scenario/lab lesson plan. The hands-on scenario/lab is presented by the intern to other cybersecurity students.

Cyber interns are selected and paired with their faculty mentors at the start of the semester. Faculty mentors work with cyber interns to select the cybersecurity tool they will work with for the semester. Throughout the semester, the faculty mentors and interns work collaboratively to develop the hands-on scenario/lab using a standard structure provided to all participants. Cyber interns and their faculty mentors work together as a group to exchange experiences and share their scenarios/labs. This collaborative work with their faculty mentor as well other interns adds to the cyber interns' experience working in groups.

According to the Chronicle of Higher Education's article, "How Colleges Can Open Powerful Educational Experiences to Everyone" internships are an experiential-learning activity that contributes to student engagement, retention, and success. Ms. Linda Buchman, director of experiential learning at the University of Georgia, reported in the article that "We know that students get more deeply engaged with what they're learning when they have a hands-on opportunity to practice." However, the article also points out that data from National Survey of Student Engagement show that "first-generation

CONTACT INFORMATION

Kasia TaylYes
ktaylor2@aacc.edu
(410) 777-7009
Anne Arundel Community College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

CYBERLEADERSHIP

CURRICULUM

DESCRIPTION

Drawing on some of the natural strengths at Texas A&M, this past semester a pilot course was taught tying together concepts of cybersecurity and leadership. Oddly though it may sound, elements of cybersecurity have synergistic leadership functions, such as looking at digital forensics and incident response, and then coupling with the situational approach to leadership. By tying these two courses together into one cohesive class, students were apply to directly apply social science leadership theory and practice to topics in cybersecurity, enhancing the learning opportunities in both disciplines.

Learning outcomes for the course included:

- Acquire the common body of knowledge in cybersecurity to include terminology, tools, concepts, and techniques.
- Demonstrate the ability to tie cybersecurity and leadership together through providing feedback and analysis to current cybersecurity topics in the global arena, specifically tailored to military applications.
- Apply cybersecurity concepts of securing networks, wireless communication, web component security, software security, and physical security.
- Demonstrate the ability to use cybersecurity and leadership fundamentals to make decisions regarding how to secure systems.

BENEFITS

With the current global need for cybersecurity professionals, while there will always be room for those in the discipline who may not want to work closely with others and work more independently, it is increasingly becoming more important to have personnel that understand leadership and the ability to work together in teams. Through this cybersecurity overview class interpolating leadership from the ground up as part of cybersecurity education, there is the opportunity to get students to think in engaged and multidisciplinary ways about how they can be the leaders of tomorrow within the field.

CONTACT INFORMATION

Daniel Ragsdale
cybersecurity@tamu.edu
(979) 845-7398
Texas A&M University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

EMBEDDING CYBERSECURITY IN GRADUATE DEGREE PROGRAMS IN COMPUTER SCIENCE AND SOFTWARE ENGINEERING

CURRICULUM

DESCRIPTION

While many institutions have focused on the development of stand-alone cybersecurity programs, the North Dakota State University has taken the less typical path of embedding options within existing graduate programs in Computer Science and Software Engineering. In making the decision to take this approach, the guiding principle was the longevity of the degree's value. We felt that teaching students core concepts in computational science and software engineering principles -- along with cybersecurity tools and core concepts -- would produce a more future-proof graduate.

The present-day acute cybersecurity need is largely caused by poor historical design, development and system administration practices. While there will clearly be an ongoing need for individuals to defend and test the defenses of software and systems, correcting the underlying design and development processes can reduce this need in the future. Individuals that have skills centered in these good development and design practices will still be in high demand, in this environment. However, there may be less demand for those whose training focuses on now out-of-date tools and practices.

To this end, we designed nine-credit options for our M.S. and Ph.D. degrees in Computer Science and Software Engineering. These options augment the strong theoretical and development foundation students receive from the core courses with immediately applicable cybersecurity knowledge and skills. Students can choose from courses on both offensive and defensive techniques, forensics and other related topics as part of this options. They can also devote additional elective credits within the degree program to additional cybersecurity study, if even more skills and knowledge in this area is desired.

BENEFITS

The key benefit to the approach that we've taken, in this area, is making more future-proof degrees for our graduates. While there are clearly core concepts and strategy to cybersecurity, many courses (in the study of programs at multiple institutions that we conducted) tend to focus on present-day technologies and issues. We are able to cover many of the relevant best practices within the core Computer Science and Software Engineering curriculums and also provide students with a broader knowledge that can make them highly valuable to work or conduct research in a larger number of areas.

CONTACT INFORMATION

Jeremy Straub
jeremy.straub@ndsu.edu
(701) 231-8196
North Dakota State University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

EXTENDING THE ONLINE CLASSROOM: RESEARCH AND PUBLIC OUTREACH

CURRICULUM

DESCRIPTION

Being able to offer research experiences found in traditional education environments to adult learners in online cybersecurity undergraduate programs is a challenge for educators. Time constraints and the nature of online programs are roadblocks. Students juggle competing work, home and academic responsibilities and priorities, and are often separated geographically, sometimes by great distances. Connecting these learners and their growing skill sets in a meaningful way enhanced the learning experience and provided a deeper connection to the institution and community.

Over 70 online students in the undergraduate Cybersecurity and Computer Forensics and Digital Investigations degree programs were tasked as information gatherers and information analysts to conduct a study of Android applications listed on Google Play's Top Charts and Excellence Award lists. The research was facilitated through a simple website, with students able to access surveys and submit responses online at designated times "after-hours" so that schedule conflicts were minimized. Data collection took place on Mondays, Thursdays and Sundays over a two-week period, with each student responsible for collecting data on the app holding a specific position on a given chart. Students were tasked with gathering and analyzing information about application developers, updates, content ratings and permissions in an effort to determine the role app developers and consumers play in data privacy. Also, students were tasked with determining whether the permissions granted during installation of each app were indicative of functionality. One student, a recent graduate who is a career changer seeking additional hands-on cybersecurity experience, is assisting with preparation of the study for publication and presentation. He is working to combine the study results with practical security/privacy advice for consumers for a national public education campaign. The preliminary results of the recently completed survey are scheduled for presentation in June 2018 during Dynamic Connections 2018, Training and Technical Forum, as part of "Security Mobility: Are You Part of the Team?"

BENEFITS

This simple and cost effective innovation utilized available resources, namely G-Suite (sites and forms features), to provide adult online students the opportunity to conduct meaningful research that will help shape future software development projects and encourage consumers to self-advocate for the protection of their privacy in cyberspace. Though developed specifically to meet the needs of this student population, the model is fully transferable to other educational settings, i.e. traditional classrooms, and to other age groups, i.e. elementary (information gatherer role) and secondary students (information analyst role). Educators can choose to ask the same questions and conduct similar research, or consider other areas of exploration.

CONTACT INFORMATION

Kathleen Hyde
khyde@champlain.edu
(802) 865-5749
Champlain College Online

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

INTERDISCIPLINARY CYBERSECURITY MODULES

CURRICULUM

DESCRIPTION

A set of twenty instructional modules, organized into four libraries covering Information Assurance, Legal Issues, Human Factors and Technical Aspects. Example topics include; Health-Information Risk-Management, Hardware-based Security and Trust, Privacy Laws and Regulations, and Political Economy of Cybersecurity.

These modules are designed to be injected into existing courses in any related discipline. The modules are designed to use one or two class periods and include presentation slides, instructor notes, activities and a brief assessment.

Interested faculty members can register to access the modules at: http://capacity.unr.edu/

BENEFITS

These modules can be used to add interdisciplinary cybersecurity content to existing courses, without dramatic changes in curriculum. This provides students with a broader knowledge base in cybersecurity and can be used to encourage students in non-technical areas to pursue cybersecurity studies related to their discipline. They can also help colleges meet the interdisciplinary requirement for NSA CAE designation.

CONTACT INFORMATION

Bill Doherty
bdoherty@tmcc.edu
(775) 673-7284
University of Nevada
Reno/Truckee Meadows Community College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

MULTI-INSTITUTION COLLABORATIVE GRADUATE CERTIFICATE IN CYBERSECURITY

CURRICULUM

DESCRIPTION

The North Dakota State University, in conjunction with two of its sister institutions within the North Dakota University System, developed a cross-institution graduate certificate program. Students can enroll in the program at any of the member institutions. They take one course each from program member institutions and a fourth course from their home institution. The certificate is awarded by their home institution.

BENEFITS

The certificate program leveraged the strength of multiple institutions and was an initial entry point into cybersecurity education for at least one of the institutions.

CONTACT INFORMATION

Kendall Nygard
webmaster@cs.ndsu.edu
(701) 231-8562
North Dakota State University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

NIST CYBERSECURITY FRAMEWORK CERTIFICATION TRAINING

CURRICULUM

DESCRIPTION

The UMass Lowell NIST Cybersecurity Framework – Controls Factory Model (NCSF-CFM) certification training program was created by Larry Wilson the CISO in the UMass president's office. The program was used to train the engineering, operations and business teams responsible for operationalizing the NIST Cybersecurity Framework controls (CIS 20 Critical Controls, ISO27002, PCI, AICPA etc.) across the university five campuses and its supply chain. The NCSF-CFM program has since been used to train other universities, governments and private corporations to do the same.

The NCSF-CFM program and its author have won the following industry awards:

- Security Magazine's Most Influential People in Security, 2016
- SANS People Who Made a Difference in Cybersecurity Award, 2013
- Information Security Executive (ISE) nominee for Executive of the Year for North America, 2013
- ISE North America Project Award Winner I for the Academic and Public-Sector Category, 2013

BENEFITS

The program teaches the knowledge, skills and abilities to:

Develop a strategy to educate executives and board members about the NIST Cybersecurity Framework (NCSF) and why they should allocate funding to launch and maintain a program; Create a Cybersecurity Program that will become policy for an organization or industry association; Engineer a solution to operationalize the cybersecurity program across an enterprise and its supply chain using the UMass Lowell NCSF Controls Factory™ Model (NCSF-CFM); Build and Operate a Security Operations Center (SOC) to continuously monitor and respond to changes in the cybersecurity profile documented in the cybersecurity program; Conduct continuous Business Risk assessments to compare the current profile against the target profile (documented in the program) to identify any gaps that need to be addressed.

CONTACT INFORMATION

Rick Lemieux
rick.lemieux@itsmsolutions.com
(401) 480-5872
UMass Lowell

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

PROGRAMMING FOR CYBERSECURITY

CURRICULUM

DESCRIPTION

Often programming requirements within Associate degree programs for Cybersecurity have limited space, which means that the number of programming courses required are general are one or none, with a max of only two. The programming courses included are traditionally the basic ones that all technology students take such as Java, C++, or Visual Basic. These courses are excellent for teaching software development foundations and language syntax, but they do not specifically address secure coding and attack and defensive coding concepts. It is often left up to the student to connect the dots between the learned language and cybersecurity concepts.

This innovation addressed this problem by creating a Programming for Cybersecurity courses at the associates degree level that would serve as a foundation programming course, yet simple enough to excite students about programming. The course has a pre-req of an Introductory Software Development course, in which pseudo-code, flow charting, and the software development cycle is learned. The Python programming language was selected as the primary language in the course because it is a simple language, yet followed object-oriented principles with some scripting features. In addition to Python, the students learned how about other languages used in the Cyber field such as: Java, C++, Ruby, Lisp, and Assembly. PowerShell was also discussed as a quick way to get data once you have access to a system. The twist is that this students are not just coding and scripting, they are also getting an introduction to some basic ciphers. They learn how to encrypt/decrypt the ciphers manually then they write programs to do the process for them. Most of these students are users of the Wireshark software, but students may not always have Wireshark available when needed, so they have to write a program with will simulate Wireshark to help them bring their programming to live and see that they can take the coding knowledge and create something on their own to solve a problem instead of always looking for the answer on the World Wide Web.

BENEFITS

The benefit of this innovation (new course) is that students learn scripting techniques for automating security tasks such as network monitoring and penetration testing using a high-level programming language common to Cybersecurity professionals. Students will also learn how to write their own custom tools and the basics of developing software exploits. They can connect their other security courses together in this course and better understand why the applications used in other courses function the way they do. Graduates with an AAS in cyber security will have General programming/software development concepts and software analytical skills, along with knowledge of Java, C++, Lisp, Ruby, Python, disassemblers, ciphers, and scripting languages PowerShell and Bash. In short, teaches programming but relates the programming to the workforce field of study.

CONTACT INFORMATION

Melissa Stange
mstange@lfcc.edu
(540) 868-7003
Lord Fairfax Community College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

PREPARING BUSINESS EXECUTIVES OF THE FUTURE

CURRICULUM

DESCRIPTION

Digital strategy drives the mission of modern organizations. Yet typical business school education does not include digital/cybersecurity strategy. Typical cybersecurity education is similarly devoid of business, leadership, and policy concepts. Traditional curriculum also includes textbooks and exams which tend to be expensive, outdated, and do not teach the skills that current employers seek. We resolved all these issues by developing a holistic graduate cybersecurity program which provides business, risk management, policy, and digital strategy elements to prepare modern executive leaders. We also eliminated all text books and exams. Instead students learn through cutting edge open source materials either readily available or custom developed by our faculty. Students complete practical real world projects which develop marketable skills and products instead of taking memory tests. Classroom materials are changed every term to maintain currency. Students learn to develop executive presentations and solid writing skills to be able to document and explain their learning to business professionals and executives.

We made the curriculum available through rich virtual classrooms and rich virtual labs accessible from anywhere in the world. This dramatically reduced the cost of the graduate program. We implemented 6 credit hour courses in order to make more efficient use of the academic calendar. Instead of hiring full-time academics, we hired a global pool of practitioner scholar adjunct faculty who have deep experiences and passion in the field to mentor and coach students.

Student get up to three attempts to successfully complete any project. This allows students to be graded on what they learned instead of what they started with. The concept allows a student to experiment, think critically, and approach the problem without fear of not getting it right the first time. Their faculty coach can help them refine an unacceptable first attempt to an excellent final product.

BENEFITS

The program results have been highly positive. The program has grown dramatically to be the largest graduate academic program in the university with over 4,000 students. The entire UMUC cybersecurity program at the graduate and undergraduate level has grown to be over 12,000 students globally. This is also most likely to be the largest cybersecurity education program in the world. The number of students who successfully complete the programs have doubled. The number of students who achieved A grades have increased dramatically because students can learn through their initial attempts, revise, and improve the quality of their work. Students can earn their Master of Science degrees in about 18 months. Their per term cost of education has decreased by about $400 each. Their entire graduate degree can be earned under $25,000 from anywhere in the world.

CONTACT INFORMATION

Dr. Mansur Hasib
mansur.hasib@umuc.edu
(240) 684-2425
UMUC - University of Maryland University College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

THE POWER OF THE SOFT TALK AND ETHICAL QUANDARY DISCUSSION AS A STIMULUS FOR CRITICAL THINKING

CURRICULUM

DESCRIPTION

What differentiates a person who has earned an Associate or Baccalaureate degree? We could say the goal skill set includes excellent technical, communication, and critical thinking skills. However, we often see professional skills and ethical judgment listed in degree outcomes as well as desired by industry. We cannot assume a person has been trained to face the ethical and critical thinking challenges in a complex role such as a cyber security professional. The actions of these individuals can impact other individuals, entire organizations, or even large populations. With the knowledge and skills comes great social responsibility. Without training in ethical decision making what is the potential result?

An expert in anything was once a beginner. We need to remember that as professors we come to this moment with years of experience and knowledge in our industry. A professor does not arrive in college with this wealth of knowledge and experience. It was acquired over many years and through ample trial and error. The primary goal of the Soft Talk is to provide knowledge of situations, conditions, and challenges that the student may not encounter for many years. A soft talk is an opportunity for the professor to share their professional and personal experience regarding a course topic. This can be introduced through current events or predetermined as part of the curriculum. This knowledge gained through assimilation over time in team level discussion in each course in each week will prepare them for the critical decision making

BENEFITS

Organizational training in ethical decision making is a great step in the right direction. But is a 5 minute ethics training presentation adequate? We should not assume that difficult decisions that can effect a thousand, hundred thousand or millions of people can be supported by the current paradigm. One course in ethics in college does not make a sound decision maker. Immersion training using soft talks and ethical quandary team discussions in each week and each course allows the student to adjust to them new perspective needed to make critical decisions.

CONTACT INFORMATION

Jeanette Smith-Perrone
jsmith-perrone@tacomacc.edu
(253) 906-9705
Tacoma Community College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

TRANSLATING HYPE, SENSATIONALISM AND EMERGING TECHNOLOGIES INTO TEACHABLE MATERIALS IN THE CLASSROOM

CURRICULUM

DESCRIPTION

Many of our college students take business, accounting courses and other non-technical or non-computer related courses, where they learn about disruptive technologies, emerging technologies and topics related to cybersecurity. Some of these topics are not found within their textbooks or traditional curriculum. Many of these topics are found in the news media, talk shows, movies and other forms of social media. These technologies are often hyped up, involved in sensationalized news and other forms of media attention that attracts and impacts our college students.

A clear example of these topics includes, but is not limited to, bitcoins, blockchains and other forms of cryptocurrencies and their profit margins.

This innovation presents an approach to incorporating emerging technologies such as bitcoins, blockchains and related cybersecurity issues within the context of a traditional Computer Science course, as well as in other programs such as Accounting, Business and Criminal Justice. This inclusion of hype and sensationalism within a traditional course is intended to demonstrate the ability to teach new and emerging topics within the context of an existing course and curriculum.

BENEFITS

Students are impacted by news about emerging technology, one way or the other. As they distill news that are hyped or filled with sensationalism, they are often unaware of the underpinnings of the technology, its true potential or its misleading promise. The incorporation of these emerging technologies, into a standard curriculum, strips the media noise and provides the students with a true feel for the underlying technology and tools.

CONTACT INFORMATION

Debasis Bhattacharya
debasisb@hawaii.edu
(808) 280-8951
University of Hawaii Maui College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

UNIQUE ANDROID APP-DRIVEN NIFTY MIDDLE-SCHOOL EDUCATIONAL MODULE ON MOBILE SECURITY FOR DRIVING BASIC INFORMATION SECURITY AWARENESS AND GENERATING INTERESTS IN CYBERSECURITY

CURRICULUM

DESCRIPTION

With the growing demand for cybersecurity workforce, as we look to prepare our youth in cybersecurity, a lack of basic awareness about mobile device security and limited practical knowledge in securing mobile devices may expose our young generation to data hacks and cyber-attacks. The current IEEE/ACM CS2013 curricular recommendations and the latest CSEC2017 cybersecurity curriculum guidelines clearly point to a need for inclusion of mobile security related topics within the present CS knowledge areas. However, even though there are limited mobile security-based curriculum development initiatives at the K-12 level, none of them focus on the theme of mobile app related permissions, vulnerabilities and exploits. Therefore, in order to address this gap in mobile security based K-12 experiential learning, we have designed and developed a unique Android app-driven information security-based learning module for educating middle-school (fifth to ninth grade) learners about relevant cybersecurity topics, like good password practices, ethics, Android app permissions, vulnerabilities, exploit-based hacking, using an Android device. Our innovative mobile security theme-driven middle-school educational module, including our original unique Android app, has been successfully used to conduct several hands-on workshop sessions for middle-school students as part of our Google IgniteCS outreach program and the NSA GenCyber camp program.

BENEFITS

Our innovative learning module, which is based on the theme of mobile-security, has the following benefits:

- creation and promotion of basic information security awareness for today's youth, including middle-school students
- generation of interests in cybersecurity, including mobile security, among pre-university youth as
- mobile security-based experiential learning model as a prospective cybersecurity educational interface for engaging youth and community
- a potential cybersecurity outreach and recruitment modular tool

CONTACT INFORMATION

Ankur Chattopadhyay
chattopa@uwgb.edu
(920) 465-5679
University of Wisconsin - Green Bay (UWGB)

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

USE OF THE RESOURCES OF STANDARDIZATION DEVELOPMENT ORGANIZATION FOR CYBERSECURITY LEARNING AND RESEARCH

CURRICULUM

DESCRIPTION

The standards are very crucial in developing Cybersecurity technologies and programs efficiently to fight against various malicious attacks over the Internet.

To satisfy this demand from Cybersecurity industry, Cybersecurity education at the college should be aligned to expose the college students to the recent and emerging security technology related standards early before their graduation. For this purpose, the education for necessity of standards, standardization procedures, and various standard development organizations and their relevant resources should be introduced to the students in teaching and learning environment of Cybersecurity courses.

I propose to use various standard development organizations' resources including NIST ITL (Information Technology Lab) Computer Security Resource Center, IETF, and IEEE more actively for teaching and research of Cybersecurity. Especially, the students can use those resources for their in-depth course research activities.

BENEFITS

The following benefits can be expected:

1. The opportunities to know about widely used standards in the security industry relevant to Cybersecurity courses can be given to the students in advance.
2. The latest standards of major standard development organizations can be accessed for Cybersecurity course research activities by the students.
3. The students can practice of acquiring and referencing faster and accurate "live" Cybersecurity standards for their learning and research.
4. The students can practice to increase their awareness about Protocol Engineering through their standards based learning and research.
5. Students can get an opportunity to understand various stands introduced in Cybersecurity courses better and apply them in their Cybersecurity study and research work and eventually for their better career management in Cybersecurity field.

CONTACT INFORMATION

Young Choi
ychoi@regent.edu
(757) 352-4949
Regent University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

02

FACULTY DEVELOPMENT

WINNING SUBMISSION:

INDUSTRIAL CONTROL SYSTEMS SECURITY CURRICULUM RESOURCE KIT

INDUSTRIAL CONTROL SYSTEMS SECURITY CURRICULUM RESOURCE KIT

FACULTY DEVELOPMENT

DESCRIPTION

In this collaborative endeavor by Jacksonville State University and Snead State Community College, an innovative industrial control systems (ICS) security portable toolkit is designed and implemented. The purpose of the toolkit is to enhance security education through total learning immersion utilizing problem based learning techniques and hands-on experimentations. The affordable (<$600) toolkit can be connected to a laboratory network switch to transform a traditional networks lab into an ICS security lab. The toolkit is supplemented with freely available ICS security curriculum modules covering topics such as ladder logic programming, Human Machine Interface (HMI) development, system reconnaissance, intrusion detection, firewall configuration, penetration testing, deep packet inspection, and vulnerability assessment. Recent enhancement to the toolkit and curriculum modules are the inclusion of virtual PLCs and scenario-based learning exercises for ICS security training.

BENEFITS

These pedagogical materials provide a novel framework for learning and teaching collaborations. Collectively, the activities and the corresponding evaluation processes for continuous improvement present a transformative educational system that is replicable at the national setting. We believe in the value of professional development in teacher retention, stimulation, and enrichment and its impact on student learning and thus, the inclusion of faculty development workshops. The ICS security curriculum modules are deployed online and evaluated as ancillary materials in courses taught by the workshop participants and the local personnel.

CONTACT INFORMATION

Guillermo Francia III
gfrancia@jsu.edu
(256) 782-5723
Jacksonville State University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

CYBERSECURITY LEARNING LABS FOR HIGH SCHOOL TEACHERS AND STUDENTS

FACULTY DEVELOPMENT

DESCRIPTION

The NSF DREAMs (Developing Rigorous and Enhanced Academic Modules) grant #170566 focuses on the development of cybersecurity lab modules which are designed to be delivered at the high school (or even middle school) level. The modules are scoped to cover narrowly defined foundational security topical areas and are timed to fit into a standard high school class period. The modules include written lab instructions at the beginner (demonstration of topic - development of knowledge), intermediate (task activity completion - development of skills), and advanced (scenario assessment and implementation - demonstrate abilities) levels for each topic. Instructor support materials include website references, Business/Enterprise and Home/Family application scenarios, Powerpoint slides, assessment questions, video demonstrations of all hands-on lab activities, and IT security certification mappings.

The lab module development goals are: (1) Foundational cybersecurity content coverage, (2) Highly standardized modular design, (3) Minimal equipment and network resources requirements, and (4) Ease of implementation by STEM and non-STEM instructors. The modules are being developed by a team which includes: high school teachers, high school students, college instructors, college students, and external technical resource personnel. An Advisory Panel of educators, business, and government representatives is providing strategic guidance and support throughout the development process. All labs are Microsoft Windows-based and require no additional software or hardware components. Lab modules can be taught serially, or in random order and are not dependent upon any prerequisite lab completion.

The lab modules are initially being developed during Summer 2018. Local (Ohio-based) training and dissemination will take place in Summer 2019 for high school teachers and college instructors, and additional remote site training will occur during Summer 2020. Development, beta-testing, and finalization of the lab modules will occur throughout the entire grant funding period.

BENEFITS

STEM and non-STEM high school teachers will have a set of resources that allow foundational cybersecurity topics to be easily introduced in their standard classes. Flexibility in the method of delivery is provided so teachers have a choice in which topics to cover, what order the topics are covered, and what level (beginner, intermediate, advanced) of coverage is appropriate. The lab module structure recognizes that high schools have different technology capabilities and available computer equipment; this will ensure that the modules can be adopted and implemented widely.

CONTACT INFORMATION

Danis Heighton
heightond@clarkstate.edu
(937) 308-6097
Clark State Community College

TRANSFERABLE

Yes, this innovation is transferable to othe institutions.

THE CYBERSECURITY EXPERIENTIAL CYCLE OF PROFESSIONAL EXPERTISE (CECPE) PRESENTS AN INNOVATIVE AND POWERFUL SEVEN STAGE MODEL OF SELF-DISCOVERY AND LEARNING LEADING TO SUCCESS FOR GRADUATE CYBERSECURITY PROFESSIONALS

FACULTY DEVELOPMENT

DESCRIPTION

Cybersecurity Experiential Cycle of Professional Expertise (CECPE) Process

Success as a cybersecurity professional is determined far more by someone's ability to do things rather than someone's ability to know things. However, one must also know things in order to be able to do things. Knowing the right things increases the chances of being able to do the right things. This is an iterative process; it is a process of perpetual learning, innovation, experimentation, observation, fine-tuning, peer and faculty feedback, and execution at progressively higher levels of success.

The seven sequential stages of the CECPE learning cycle continuously strengthen the professional expertise and execution skills of cybersecurity professionals, students and digital forensics examiners in our graduate programs. The process is open and welcomes graduate students from all backgrounds and has successfully allowed high levels of gender and racial inclusion and a diversity of ideas into the profession, while removing artificial entry barriers.

As students go through this experiential cycle, they discover what they enjoy and what they are good at. People naturally do better in doing things they enjoy. They also discover the strengths and weaknesses of the people around them to help improve outcomes. They learn to collaborate by applying the collective strengths of all the expertise around them to execute the strongest solution to any problem. An engaging seven stage diagram depicts the dynamic competency-based model of learning at the UMUC Graduate School Cybersecurity Program.

BENEFITS

Embracing the innovative Cybersecurity Experiential Cycle of Professional Expertise as a perennial process is the foundation for a dynamic and rewarding career as a cybersecurity professional. After completing the Cybersecurity Experiential Cycle of Professional Expertise, students are professionally poised, well-trained and strongly equipped to begin a new experiential professional cycle of excellence in the cybersecurity field.

CONTACT INFORMATION

Patrick O'Guinn
patrick.oguinn@umuc.edu
(240) 684-2071
University of Maryland University College Graduate School

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

03

LAB ACTIVITY

WINNING SUBMISSION:

HAVE MY SMART LIGHTBULBS BEEN WEAPONIZED: INTRODUCING COMPUTER SECURITY ISSUES RELATED TO IOT DEVICES

HAVE MY SMART LIGHTBULBS BEEN WEAPONIZED: INTRODUCING COMPUTER SECURITY ISSUES RELATED TO IOT DEVICES

LAB ACTIVITY

DESCRIPTION

A current issue plaguing the information security industry is poorly designed, misconfigured Internet of Things (IoT) devices found in the home. To address this issue students created their own IoT device and analyzed the security implications of their design.

Students used a Raspberry Pi and a motion sensor to create their IoT device. The concept is to write a program on the Pi that will send a text alert whenever the motion sensor is triggered. The method to implement this functionality includes interfacing with an external third-party website which generates a text. This architecture is typical of a IoT device; IoTs typically receive input from a sensor and then relay that event to an external website.

Students also used a personal mini router to learn about network traffic. First, they utilized a tool on their router to monitor traffic generated by their Raspberry Pi. This establishes a normal baseline of traffic. Next, they wrote their own program in Python to create an alert whenever their Raspberry Pi deviated from the established norm, this indicated anomalous traffic.

BENEFITS

Incorporating real world security problems in which the students are actively engaged in solving the problem, produces better mastery of and interest in the subject material. It is important to focus the project on a problem that directly effects the student and provides a solution that they can create and implement.

CONTACT INFORMATION

David Zeichick
dzeichick@csuchico.edu
(530) 592-6001
CSU, Chico

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

AN AUGMENTED STUDENT LEARNING AID FOR ETHICAL HACKING COURSE

LAB ACTIVITY

DESCRIPTION

The game lab innovation is an inclusion of cyber defense tactics with cyber offense tactics as an exercise demonstrating expertise in understanding vulnerabilities and potential threats to a system. This innovation requires a red team and blue team integrated approach in portraying the attack phase and defense measures in a lab environment. The lab is virtual and the phases include a scenario of attack options with defense action options that may be immediately selected and applied to respond to the exploitation. The inclusion of this fast-paced and engaging game lab provides practice in typical on-the-job scenarios. Students will engage in offense and defense in this game lab and the interaction is quick with choice remedies from attack to defense. The lab is isolated and will not use the actual tools necessary for a penetration test however; the simulation is based on the behavior of the tools.

A simulated tool resource option may be selected to respond to an attack. A legend that describes the attack type is provided. The student then selects the proper remedy of defense for this attack type. A defense legend of options appears and the student applies the incident response measure and appropriate control based on the configuration. The game will engage the student in 25 exercises which require reaction and timing to attacks. This is an augmented exercise for ethical hacking. The game lab requires a virtualized environment and Microsoft software was used to develop this game lab. It was written in Visual Basic and is a simple game construction simulating an environment.

BENEFITS

Ethical hacking is an essential skill in protecting our infrastructure whether military, government, healthcare, industry, and/or academic institution. In understanding the attack and associated remedy. Student knowledge is enhanced with the practical and immediate decision-making requirements in the game lab. This reinforcement of operational knowledge adds to the skill of the student and builds confidence in applying the knowledge learned in the course.

CONTACT INFORMATION

Nancy Landreville
nancy.landreville@faculty.umuc.edu
(304) 707-4812
University of Maryland, UC

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

CLOUD-BASED, AI-POWERED, FULLY IMMERSIVE CYBER RANGE/ CYBER SECURITY TRAINING, EDUCATION AND ASSESSMENT SOLUTION

LAB ACTIVITY

DESCRIPTION

Circadence® Project Ares®, the only gamified, artificial intelligence (AI) powered cyber training solution, changes the paradigm for cybersecurity education by engaging learners interested in or pursuing a CS/cyber-focused path by utilizing real-world tools and tactics in immersive, virtual environments.

Students at all levels of proficiency have access to an evolving library of mission scenarios and modern educational resources in a hands-on, gamified environment that brings the static classroom to life. They work alone or in teams to stop hackers, protect systems, and hone their skills inside environments that mirror the actual businesses and organizations they will defend in their future careers. This approach encourages the repetition necessary to develop lasting skill and knowledge retention, while keeping students excited and engaged.

BENEFITS

Our virtual gaming environment adapts to the experiential learning style of next generation students, and supports customized, task-oriented training, skill-specific games, and mission scenarios for both individual and team-based exercises. Students have the opportunity to prepare in the Project Ares Battle School, which enables asynchronous practice and review of cyber skills and knowledge. Key features include: cyber games for technical topics (i.e. Cylitaire, PortFlow), battle room for non-mission specific tactical practice, and a media center for videos, documents, and other key resources/websites in cybersecurity. Scenario-based missions and game play enable users to earn skill badges and certifications as expressions of their proficiency on singular cyber tasks and in large-scale, cooperative settings. These badges and certificates encourage progress and serve students long-term as notes of accomplishment to be highlighted on applications for internships, furthering their education, and pursuing their careers.

CONTACT INFORMATION

Bradley Wolfenden
bwolfenden@circadence.com
(858) 208-8003
Circadence Corporation

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

CYBER SECURITY ANALYST SIMU-LAB SUITE: DEVELOPED BY ISRAELI MILITARY OFFICIALS AND EDUCATION EXPERTS WHO DESIGNED THE PROGRAM TO PREPARE STUDENTS FOR CYBER SECURITY ANALYST POSITIONS

LAB ACTIVITY

DESCRIPTION

The Cyber Security Analyst Simu-Lab Suite is the product of extensive military and industry experience, which offers advanced practical training in a virtual machine environment. The CSA Simu-Lab Suite is comprised of 10 labs that bring a much-needed practical work experience component to students.

Each lab is based on an authentic real-life cyber incident that learners will practice solving using cyber tools through a simulated virtual machine. We want students to feel as if they are in a real Security Operations Center (SOC) and to work as Cyber Security Analysts (CSA).

Our goal is to provide learners with a solid foundation that will prepare them for on-the-job training and allow them to grow professionally. This comprehensive offering allows participants to quickly gain the skills and experience to start working in the cyber industry – even without a computer science degree.

BENEFITS

- Hands-on simulated work experience
- Provides skills required for Cyber Security Analyst positions in the workforce
- Enhances student problem solving and decision making abilities
- Certification of completion strengthens resume

CONTACT INFORMATION

Devon Milkovich
devon.milkovich@cybintsolutions.com
(212) 719-0748
Cybint Solutions

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

INTRANET SECURITY POLICY PROJECT LAB ACTIVITY

LAB ACTIVITY

DESCRIPTION

To understand why cybersecurity is important, it is essential to understand both the value of information and the consequences of such information being compromised.

The purpose of this Intranet Security Policy Project lab activity is to provide students hands-on, real-world experience with creating or modifying security policies. This lab activity allows students the opportunity to learn about security policies, HTML, and the Internet. The recommended time to complete this project is about 3 to 4 weeks.

Students will use a fictional company and create or modify security policies to support that company. The security policy templates may be provided by the instructor or students may be required to create their own (normally seven to ten security policy is recommended). Next, students are required to create an Intranet site. The site includes information about the company, company vision or purpose, mission statement, and selected security policies, and a frequently asked question (FAQ) page. Additional links may be provided to support the project. The project must be developed using HTML or a web authoring tool. No online web development tool is allowed. After completing this project, students will have a better understanding of how to create or modify security policies based on best practices.

BENEFITS

The benefit of the Intranet Security Policy Project lab activity is to provide students the opportunity to obtain hands-on, real-world experience with creating or modifying security policies. The development of security policies may seem easy, but security policies should be well written, clear, and support the mission of the company. Security policies should be addressed in all cybersecurity curriculum. This Intranet Security Policy Project lab activity can also serve as a capstone project for a Fundamentals or Information Security course. This project has been used at Tarrant County College, Southeast Campus for the past five years.

CONTACT INFORMATION

Dr. Charles DeSassure
charles.desassure@tccd.edu
(817) 515-3737
Tarrant County College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

MYSECURITYLAB: A GENERIC TOOL FOR SELF-PACED LEARNING OF SECURITY CONTROLS

LAB ACTIVITY

DESCRIPTION

Cybersecurity students and security staff members in industry all require adequate knowledge of operational software safeguards, network defense and applied cryptography. Unfortunately, the in-depth understanding of security techniques and mechanisms require more mathematical ideas beyond discrete math and calculus. Moreover, most students come across learning difficulties in courses such as applied cryptography and open systems interconnection layers security.

MySecurityLab is an interactive tool with a graphical user interface that provides instructions and practice modules for self-paced learning of (1) elements of modulus arithmetic and number theory; (2) symmetric and asymmetric algorithms for providing data confidentiality, nonrepudiation, key exchange, and digital signatures; (3) hashing algorithms for providing data integrity; (4) scripts to set up alternative DevOps tools for monitoring and analyzing the security of networks; and (5) scripts for setting up access control lists.

BENEFITS

Cybersecurity students and employees in organizations can use this tool for self-paced learning of the administration of technical security controls in stand-alone and network systems. The self-paced learning tool will enable current and future cybersecurity professionals to achieve proficiency in the applications of technical security mechanisms. Faculty members can use the tool to effectively teach cybersecurity courses and make learning more sensational!

CONTACT INFORMATION

Amos O Olagunju & Ananda Poudel
aoolagunju@stcloudstate.edu
(320) 308-5696
St Cloud State University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

SECURING THE COLLEGE COMMUNITY OF STUDENTS, FACULTY, AND STAFF AT A CYBER SECURITY AND AWARENESS FAIR DURING NATIONAL CYBER SECURITY AWARENESS MONTH

LAB ACTIVITY

DESCRIPTION

A Cyber Security and Awareness Fair is held at Cal Poly Pomona every October as part of National Cyber Security Awareness month. The mission of the event is to educate the college community on cyber security topics with an interactive environment surrounded by peers and industry experts. The fair is constructed so that the college community are engaging in spirited learning with regard to all aspects of technology and security, hardware, cracking, privacy, crime, fraud, and social implications.

The committee responsible for the event are faculty, staff, professional association, and student club leadership from Cal Poly Pomona, Fullerton College, Coastline Community College, and ISACA Los Angeles. The fair has three components. One component is industry speakers discussing a hot topic appealing to an audience of all skill levels. The second component are villages run by the student clubs with hands on activities for attendees. For example, in 2017, one village was titled "Don't Take the Bait! The dangers of phishing attacks on WiFi users" where a student club presented an interactive demo on how cyber criminals can use "phishing" or social engineering techniques to con unauthorized access to WiFi, coax out email addresses and Facebook passwords, deliver spyware, and worse!

The last component is a student poster competition. Full-time undergraduate and graduate students are encouraged to submit poster presentations on emerging topics in the field of cyber security, information assurance and forensics. Poster abstracts are submitted to a blind review to determine acceptance. Thanks to the Los Angeles Chapter of ISACA, poster competition winners were awarded monetary prizes. The 2017 grand prize security research poster contest winner out of 43 entries was from Fullerton College. The topic covered Webcams Impact and Consequences on Mainstream Life.

BENEFITS

In 2017, over 400 participants from Cal Poly Pomona, Fullerton College, Coastline Community College, Chaffey College, and Charter Oak High were exposed to information technology security awareness. Students clubs gained experience on sharing their knowledge by providing hands on peer-to-peer mentoring with security concepts. Students were provided opportunities to speak with industry leaders about new technologies and professional associations like ISACA on how to keep abreast of security issues. The industry partners support of donations, exhibits and presentations provides a promotional benefit of a personal introduction of their company with staff, faculty and students that will soon be influential buyers or employee.

CONTACT INFORMATION

Anna Carlin
acarlin@fullcoll.edu
(909) 896-4567
Fullerton College, Cal Poly Pomona, and Coastline Community College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

SECURITY POLICIES: HOW TO ENGAGE STUDENTS IN THE LEARNING PROCESS

LAB ACTIVITY

DESCRIPTION

One component that cannot be overlooked in the area of cybersecurity is security policies. Research shows that security policies may help reduce threats to an organization. We as educators talk about security policies regularly, read about security policies in textbooks, and explain to students how important security policies are to an organization. But the question is, do our students thoroughly understand the value of security policies? The purpose of this real-world, hands-on lab activity is to provide students with the opportunity to create or modify security policies.

Students are responsible for creating a functional intranet site for a fictional company. An intranet is a private network belonging to an organization, usually a corporation, accessible only by the organization's employees or others with authorization. Students are required to use pure HTML code and web authoring tools. No online web development tool is allowed. Once the student project has been completed, students will submit a USB drive or CD-ROM with all required files for their functional intranet project. For this lab activity, I recommend using a grading rubric. The final project should include a company history, mission statement, service or product provided by the company, security policies to reflect the environment of the company, and a Frequently Asked Question (FAQ) page with at least five general-purpose questions and answers. Some of these items may be changed, renamed, or deleted, or additional links can be included—it is up to the instructor. The security policies for the intranet may be provided by the instructor, or students may be required to research and write their own security policies for their company. I recommend a total of ten different security policies to support the company, but this number can be changed by the instructor. The timeframe to complete this security intranet policy project is about 3 to 5 weeks.

BENEFITS

The student learning objective (SLO) for this lab activity is for students to be able to create or modify security policies for a fictional company. This lab activity is designed to provide students with real-world, hands-on experience related to security policies to support a company. Students also learn more about the internet, HTML, and web development. This project also may help students develop their organizational skills. The instructions for this lab activity can be used in a face-to-face, online, hybrid, or blended learning environment. This lab activity is suitable for the first-level Introduction to Security or Cybersecurity course.

CONTACT INFORMATION

Charles DeSassure
charles.desassure@tccd.edu
(817) 515-3747
Tarrant County College, Southeast Campus

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

THE SPLUNK PLEDGE

LAB ACTIVITY

DESCRIPTION

Splunk (a company recognized by the Gartner organization as one of the leading providers of security SIEM solutions) has developed and implemented the Splunk Pledge Program. This program provides a no cost Splunk license, full semester curriculum, and access to Splunk training for both instructors and students in higher education institutions that want to incorporate Splunk into their cybersecurity curriculum. Additionally, the program allows students to test for Splunk User and Splunk Power User certification at no cost, following completion of the core modules required prior to taking the certification exams.

BENEFITS

Allows higher education institutions to incorporate leading edge cybersecurity technology into their program curriculum. Allows the institution to establish a Splunk instance that can be used by students to complete labs and work that is directly related to their course(s). It also allows students to obtain certifications that are in very high demand in today's rapidly changing technology/cybersecurity career/workforce environment.

CONTACT INFORMATION

Richard Seidner
rseidner@splunk.com
(215) 378-4110
Splunk Incorporated

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

UCC OFFERS A CYBERSECURITY DEGREE WITH OPTIONAL LAB ATTENDANCE BASED ON CUTTING-EDGE TECHNOLOGY AND EQUIPMENT

LAB ACTIVITY

DESCRIPTION

While our degree can be taken 100% online, we hire students to staff our labs where real-world equipment such as racks, cabling, routers, switches, and servers are available for their use. Our students workers assist in training the other students to reinforce learning. Instructors are fully trained in each of the courses they teach, and in most, if not all instances hold the applicable valid industry certifications.

Most of our courses are reinforced through the use of video lecture series that are specific to each course.

BENEFITS

Students have access to actual equipment meaning that while they learn course theory, they also have access to equipment similar to what they will use upon graduation. Further, after learning the material from their instructor, student-to-student learning reinforces concepts learned through repetition.

CONTACT INFORMATION

John Blackwood
john.blackwood@umpqua.edu
(541) 440-7686
Umpqua Community College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

USING AN EXTENSIVE CASE STUDY IN THE COMPUTER INFORMATION TECHNOLOGY (CIT) CAPSTONE CLASS

LAB ACTIVITY

DESCRIPTION

The Capstone Class in the infrastructure concentrations at Pellissippi State Community College included students from three CIT concentrations: Systems Administration and Management, Networking and Communications, and Cyber Defense. Students from each concentration were assigned to each "team" so that each "team" was comprised of a mix of students who were graduating spring semester 2018. The case study was composed of an extensive Request for Proposal (RFP) that required the analysis of a physical building plan for a new facility consisting of a "design department with product design engineers", a "server infrastructure data center", and a "multipurpose room" that required a wireless infrastructure that was completely isolated from the adjoining CEO suite of offices. In addition to the physical secure networking and wireless communications facility, the data center consisted of a SAN of specified data density (275TB) along with a file server, database server, web server, and other specified hardware and software requirements. All of these items including the type, brand, and associated costs were the responsibility of each "team" which represented separate companies each of which submitted their responses to the RFP. Each "team" was also given the responsibility of providing their plans for installation (including detailed time-lines), staffing the installation, and providing the overall plans for system acceptance testing and security after the installation was complete. At the end of the allotted time for the RFP submission, an extensive written "bid" was submitted for their solution along with a public presentation (20 minutes for each presentation). This presentation was graded by invited members of the college's Information Technology staff along with information technology professionals from the community.

BENEFITS

Spring semester 2018 was the first time this class had been offered at Pellissippi State Community College. The CIT Infrastructure Concentrations Capstone class completed an extensive 15-week Lab Activity that far exceeded the typical community college assignments both in breadth and depth. This "Lab Activity" required the use of all classes each student in the three concentrations had completed in preparation for graduation: hardware, software, networking fundamentals, Windows client and servers, Linux, wireless technologies, routing and switching, virtualization, information assurance, network security, system forensics, and perimeter protection. The class was also a "Student Learning Aid" since no single class or previous combination of classes had prepared any of the students for such a large managed project like they may face in their future careers. This class was also a "Local Partnership" since local information technology (I.T) professionals had the opportunity to view first-hand the skills and knowledge of these graduating students in the CIT Infrastructure Concentration. Most of the invited professional I.T. executives did not know the capabilities of these graduates since this is a new degree concentration at the College. After the presentations, we now have additional members of the community who have asked to serve on our curriculum advisory committee!

CONTACT INFORMATION

Bradley Wolfenden
bwolfenden@circadence.com
(858) 208-8003
Circadence Corporation

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

VIRTUAL MACHINES FOR CYBERSECURITY TESTING

LAB ACTIVITY

DESCRIPTION

AWC has incorporated virtual machines into the classroom for networking and cybersecurity. The students are able to work in a safe, sandboxed environment that matches the real world operating system for labs and do any assignments they can do on ''real'' computers. Included on the machines are open source, freeware, and bundled with the text software for the students to use in their work.

BENEFITS

1. Students are segregated from the live network to prevent contamination.
2. Students are able to take their work home with them and continue the labs or other assignments from where they paused.
3. Copies of the students' work can be made without interfering with the work they are continuing to do.

CONTACT INFORMATION

David Parker
david.parker@azwestern.edu
(928) 317-6261
Arizona Western College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

04

LOCAL PARTNERSHIP

WINNING SUBMISSION:
GUIDING GIRL SCOUTS THROUGH A COMPUTER SCIENCE JOURNEY

GUIDING GIRL SCOUTS THROUGH A COMPUTER SCIENCE JOURNEY

LOCAL PARTNERSHIP

DESCRIPTION

On May 7, 2017, former NASA engineer Sylvia Acevedo was named the new CEO of the Girl Scouts of America. She immediately made it clear that she was an advocate of STEM education for young women by releasing several new badges and three new journeys, including one for computer science. Gulf Coast State College's cybersecurity-focused student organization and cyber demonstration team, Corps Tigris, saw this as an opportunity to assist the local Girl Scout Service Unit. If successful, more than 100 scouts, in grades K-5, would complete the requirements for the "Think Like a Programmer" Journey badge. For the kindergarten-age Daisies it would be Girl Scout history as this was the first time the youngest of scouts got an opportunity to earn this kind of award - which they did on October 21, 2017.

So, how did we do it? Well, we needed an interactive, engaging, and entertaining day of events following the Girl Scout's requirements. The challenge was morphing the complex world of programming, cybersecurity, and IT into something that could capture the imagination of digital native girls in grades K-5. We leaned on material from the Department of Homeland Security (Stop Think Connect) to explain online safety. The girls used this presentation to create their Service Learning Project - a poster to share with others about what they just learned. We introduced them to Python coding, which we used to create a live cell phone "hacking" demonstration - the thing the "Tigers" do best. We led a discussion of how we developed and delivered the code to a cellular phone, including the owner's role in the social engineering attack required to load the malware. We recycled old keyboards for the day's craft to show a socially responsible way to reuse "old tech" and invented a matching-style card game to teach debugging. One card was simple ones and zeroes - good code. Another featured a roach - a bug that needed another "card" to patch it. Occasionally someone would find a mouse - representing malware and it too required a "patch" to eliminate the problem. The cards are created in Publisher and available for free use by any Girl Scout unit.

Our greatest feat was teaching the complexity of designing a program so a robot could do a simple task. In order to "Build Al Gorilla's Sandwich" - featuring bananas and peanut-butter slammed between two slices of bread - the scouts had to develop a step-by-step set of instructions with the aid of an instructor. Another instructor played a very dense robot who took their "commands" quite literally. Merely shouting "drop plate" could send everything crashing to the floor, instead of the table with its 3x3 grid. Soon the girls learned to call out grid coordinates like bingo numbers, which led the robot into the right direction for ingredients and the final placement of the finished product. In this exercise they learned about algorithms, functions, commands, variables, and structures. They discovered that the more detailed their instructions, the better the outcome. As they worked through the inevitable problems - try telling a robot how to open a jar of peanut butter - they discovered the depth and breadth of thinking required to produce workable code. Again, we detailed this event and made it available to any GSA unit with coaching tips for the volunteers who might decide to try it - no computer science experience required.

See page 35...

GUIDING GIRL SCOUTS THROUGH A COMPUTER SCIENCE JOURNEY (cont.)

LOCAL PARTNERSHIP

BENEFITS

By developing interactive and inexpensive training programs, we decoded the complexity of designing and developing a computer program. The simplicity of a match-card game to crystallize the debugging process gave each girl an opportunity to take her first steps into the realm of software engineering. We connected the entire day with a bias towards active learning and made "geek into chic." The instant reward of solving a problem, like getting that silly robot to put the plate on B2 instead of the floor, complimented the "wow" factor of watching one of our female cybersecurity students lead a hacking attack. For the Tiger team, delivering content for an entire day to an audience this young was quite new. Each of them had to break down complex concepts in an almost Disneyesque way. In addition, the scouts spent time with our female cyber students, who were living examples of what each of them could be when "they grow up." The program received excellent reviews and will be repeated by Corps Tigris in the next academic year.

CONTACT INFORMATION

Guy Garrett
ggarrett@gulfcoast.edu
(615) 351-2853
Gulf Coast State College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

ACCESSCYBER

LOCAL PARTNERSHIP

DESCRIPTION

AccessCYBER aligns industry and academic partnerships to bring students and professionals under one roof as they analyze recent data breaches (from a technical, legal, communications, public relations perspective) and work together to present their findings and best practices. Students work in groups to approach cyber incidents through the analytical lens of journalism, as they assess the means, motive, and method of an attack, determine risk, identify attack vectors, explain the difference between targets and victims, estimate damage beyond financial loss, and communicate with stakeholders through professionally crafted breach disclosure notices. Furthermore, these students serve as 'Cybersecurity Ambassadors', volunteering to share their knowledge of 'cyber hygiene' best practices with middle and high school students through gamification platforms. Lastly, the AccessCYBER.org website, contains a list of free resources available that can be used for independent self-study, school cyberclubs, or instructor-facilitated learning.

BENEFITS

AccessCYBER supplements traditional classroom experience by introducing real-world scenarios that affect us all - serving to reinforce the notion that digital actions often have consequences in the physical world. By working directly with industry mentors, students are exposed to a variety of careers in infosec and gain a better understanding of what specific careers they are interested in pursuing.

CONTACT INFORMATION

Gotham Sharma
gotham@exeltek.net
(347) 801-3936
AccessCyber.org

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

ADVISORY BOARD AND LOCAL INDUSTRY PARTNERSHIPS

LOCAL PARTNERSHIP

DESCRIPTION

Bossier Parish Community College has worked hard to build a solid partnership with local industry. We have MOUs with over 30 local IT related companies that enable us to "tap" their resources. We feel that solid local partnerships are a MUST. They are the ones that will hire our students once they complete our program of study. So we need to be sure that we are on track with the skills that they need for the work force of tomorrow. This is done in multiple ways. First, internships. Each of our program have a capstone internship requirement. These are competitive placements, meaning that the students do not choose who they want to work for, industry chooses which student they want to intern with them. In this manner it pushes the students to strive in their programs of study to secure the higher level internships. Every student entering the internship must hold at least one national level certification (ie CompTIA, Net+, Security+, CCNA, etc). Secondly, Partnerships. As already mentioned we have over 30 MOUs for local partnerships. In addition to these we have our advisory board. Each year we meet to discuss what is good, what can improve, and what needs change. We have found that this works great as a round table discussion where we can address key areas and allow a free flow of thought. Our board knows that they can contact us throughout the year with questions/insight. As a community college we are able to adapt to industry needs quickly. However, we do not tailor a course to just one industry. The courses that are designed must benefit the collective not just the one.

BENEFITS

Key benefits of Internships:

Students get real life experience in a production environment
Students are mentored by industry parnter
Students have job experience that can now be listed on their resume
Industry get to be part of the learning expereince
Industry can provide feedback on skills for students in the internship to provide insight on what needs to happen to improve our program

Key benefits of Industry Partnerships:

Industry provides insight on training that is needed for a skilled work force
Industry provides connection of topics covered in our courses to real life application
Industry provides hands on training for our students (their future work force)

CONTACT INFORMATION

Chris Rondeau
crondeau@bpcc.edu
(318) 678-6317
Bossier Parish Community College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

CENTER FOR CYBERSECURITY AND TECHNOLOGY AT SUNY PLATTSBURGH

LOCAL PARTNERSHIP

DESCRIPTION

"is a collaboration between the Management, Information Systems and Analytics (MISA) Department and Computer Science Department faculty. The center hosts cybersecurity projects and research to offer students hands-on opportunities to practice skills learned in the classroom. Students from the Cybersecurity Track in MIS and from computer security majors are interning at the center. The center conducts an outreach program to local high schools to encourage students to pursue careers in cybersecurity by engaging them in projects with their college peers. In addition, the center is a resource for all things cyber for local businesses and non-profit organizations. A think tank of sorts, the CCT is a "go-to" place for START-UP NY businesses to engage with our students, host internships, and get information about the technology infrastructure available in the North Country.

With the CCT, the college added the necessary hands-on, practical experience that students need in addition to classroom learning. Adding to our existing infrastructure, which includes an MIS and a computer science lab, the center has flexible computer network managed by the student interns. Currently, students are working on configuring firewalls, intrusion detection systems (IDS), network monitoring, and setting up a malware analysis virtual lab. Future expansion will include digital forensics platforms to support our local law enforcement partners.

The center is dedicated to a strong relationship with the business community, to directly support and provide qualified candidates for future cyber positions in the industry. The governance of the CCT is composed of members from the business community with interest in cyber and information systems along with our cyber/information system faculty and START-UP NY representative. Student interns have the infrastructure to experiment with security tools and "legally hack" without causing any permanent damage to a network. While experimenting and testing commercially available security tools, the center makes a commitment to open source tools development. Interns join the Open Source community in building security tools that are freely available on the Internet. Currently the center in its third semester has over 35 interns. Our first class is graduating and already we are seeing our interns getting high paying jobs in the industry. https://web.plattsburgh.edu/offices/academic/cct/index.php. Offer students internships in Cybersecurity, outreach to encourage high schools student to consider cyber career field, community outreach and cyber awareness, think tank for cyber for both academic and local community, create "buzz" about cyber, opportunity for students to join in on open source projects, opportunity for students to work with industry cyber tools, flexible network to experiment. Make a proverbial "home" for students interested in cybersecurity where they can meet with like-minded cyber "geeks."

CONTACT INFORMATION

Cristian Balan
balanc@plattsburgh.edu
(518) 569-1423
SUNY at Plattsburgh

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

COMMUNITY COLLEGIATE CYBER DEFENSE TEAM

LOCAL PARTNERSHIP

DESCRIPTION

Several groups from around the Bismarck, ND community teamed up to form the first ever Collegiate Cyber Defense Competition Team (CCDC) for the area. The idea was started by Col. Ray Knutson of the Army National Guard who had attended the CCDC competition the year before. He saw the value in the competition and knew that North Dakota needed to have a team compete. Contacts were made, and through a joint effort of Bismarck State College and the University of Mary in Bismarck, a team was formed. 4 students from each school joined the team to compete in the regional CCDC competition.

The collaboration didn't' stop there though. To prepare the students for the competition, we reached out to industry to ask local professionals if they would be willing to come give presentations. The presentations focused on showing students what to look for during the competition and how to go about responding to the incidents that happen during the competition. We had professionals from private industry, the State of North Dakota cybersecurity department, and the Army National Guard all give presentations. Most presentations included hands on lab activities to reinforce the skills being taught.

BENEFITS

The benefits were amazing! The team placed 3rd in the regional competition which gave them a great sense of pride and accomplishment. They brought that pride back into the classroom and shared their experience with the other students. This created quite the "buzz" in the programs at the schools, and students are already looking forward to next year. Students were able to take what they learned in class and apply it during the competition. It reinforced the skills they learn in class and during the industry professional presentations. It challenged them to think in different ways and forced them to build a team and relationships with people outside of their day to day interactions. We are so happy that we all took on the challenge of doing this joint effort, it exceed our expectations!

CONTACT INFORMATION

Matt Frohlich
matthew.frohlich@bismarckstate.edu
(701) 224-5581
Bismarck State College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

CYBERLIABILITY ONLINE COURSE

LOCAL PARTNERSHIP

DESCRIPTION

Business/education partnership - Partnership between Ohio Dominican University faculty and an insurance industry cooperative organization (Associated Risk Managers, a group of approximately 200 agencies in the U.S. generating $5 billion dollars of insurance premiums).

1. Raises awareness and expertise of cyber risks and potential to allow risk transfer throught the use of cyber liability policies from for- and not-for-profit enterprises to insurance carriers, benefitting both insurance professionals and risk management professionals in all industries and organizations.

2. Prepares undergraduate students for post-college employment in cyber risk management or insurance by providing a certification in the cyber liability specialization (Cyber Risk Manager -cyRM(c)). The cyRM Course jump-starts learning for students on evolving IT perils. Experts say cyber risks will come to dominate business risk perils; this program is a step towards a learning process that must continue for the balance of students' careers. Currently nationwide in the USA, India and Canada.

BENEFITS

This course exposes the student to the topic of cyber liability, cyber security, client service, and career development. The course provides students knowlege for developing cyber risk perils that affect virtually every commercial insurance customer. This online course is a careful curriculum weave of cybersecurity and risk management education designed for both professionals and students. With training students learn to address this crucial business risk, and then effectively integrate cyber insurance to their customer services. The course is 100% Online – No textbooks, study guides, or extra purchases necessary. A certification test ensures Graduates have acquired knowledge, and are prepared for speaking with clients about the basics of cyber insurance.

CONTACT INFORMATION

Douglas Ruml
rumld@ohiodominican.edu
(614) 432-1729
Ohio Dominican University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

HARRISBURG UNIVERSITY OF SCIENCE AND TECHNOLOGY'S, SECURITY CENTER OF EXCELLENCE, CHIEF INFORMATION SECURITY OFFICER (CISO) CERTIFICATE PROGRAM

LOCAL PARTNERSHIP

DESCRIPTION

Harrisburg University of Science and Technology (HU) established a Security Center of Excellence (SCE). The center is a targeted effort to support government security leaders and their staffs as well as the private sector through educational programs, collaboration and awareness-raising initiatives. HU leverages its faculty, students and business partners to connect Information Security professionals with the latest, best practices and technologies. Through its partnerships with leading technology and security companies, the business community, technology associations and educational institutions, the center brings together a robust community of stakeholders and contributors in support of a shared mission.

Chief Information Security Officer Certificate Program Overview

HU's SCE, Chief Information Security Officer (CISO) Certificate provides a unique focus on leadership in the area of information security for IT professionals. It enables IT leaders responsible for information security to further develop the knowledge and skills necessary to succeed at the executive level.

BENEFITS

Through strategic partnerships with PA State Government, private sector security companies and Harrisburg University's faculty and students, the CISO Certification Program prepares individuals to perform the primary responsibilities of a Chief Information Security Officer (CISO). Application of these skills to the performance of security management will be emphasized. The program will help develop the skills and knowledge needed to: Provide strategic leadership as a steward of the organization's information security and a trusted partner with other business executives in the organization; Develop and implement a robust, accurate, and actionable metrics reporting process that maps back to the business; Understand and manage the risk posture of an organization. Communicate and work closely with legal and privacy officers to protect the organization from legal and regulatory non-compliance. Establish and manage an IT security strategy for the organization that maps to the business objectives and lifecycle. Establish and manage the organization's security policy catalog. Understand requirements for secure development lifecycle, and application security concepts. Understand and manage the security implications of emerging technologies. Secure adequate resources, and manage the IT Security budget. Lead and manage a technical staff of security managers, architects, engineers and specialists, as well as contractors and vendors.

CONTACT INFORMATION

Kelly Logan
Klogan@HarrisburgU.edu
(717) 901-5171
Harrisburg University of Science and Technology

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

METASPLOITABLE 3: A WIN-WIN SITUATION

LOCAL PARTNERSHIP

DESCRIPTION

Metaspoitable 3 is gaining popularity as the de facto VM environment which students have to configure and exploit vulnerabilities. Students will explore how to do penetration testing similar to a real world penetration testing experience. High School students in the Oak Ridge Area were provided limited information on how to set up a lab with Metaspoitble 3 using VirtualBox. They were divided into teams to see which team will set up their lab first. Then the winning team not only will showcase their set up to the rest of the teams but also will share the difficulties faced with the different Virtual Box versions, Vagrant, and Packer they downloaded

Afterwards the teams were divided into two groups:

1. Exploitation Team: Network Discovery using ARP, netdiscover, nmap, db_nmap, and scanning for different ports including the UDP ports, user accounts on the target machine.
2. Post Exploitation Team: Once access has been made available on the target machine, all different vulnerabilities have been exploited. Students located the exploits, discussed the exploits, ranging from database and SQL injection to downloading PowerSploit. The latter being A Windows privilege escalation framework. They concluded by comparing the kinds of privileges they were able to explore because of PowerSploit and Catch the flags in Metaspoitable3.

Students considered the above as their reason for choosing a career in cybersecurity and enroll in a concentration for cybersecurity: A win-win situation for all involved.

BENEFITS

Immersing High School students in a virtual environment like Metaspoitable 3 provided them with the opportunity to explore vulnerabilities, and discuss vulnerabilities. The experience proved to be life changing. Students now look differently at cyber security and consider it the best area in technology they that will embrace. Because of Metaspoitable 3, they are now researching vulnerabilities at all levels including devices, PLC, and internet connected things.

CONTACT INFORMATION

George Meghabghab
meghabghagv@roanestate.edu
(865) 556-5257
Roane State Community College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

NATIONAL CYBERSECURITY CAREER AWARENESS WEEK SPEAKER SERIES - THREE PHASE PRESENTATION MODEL

LOCAL PARTNERSHIP

DESCRIPTION

We invited multiple speakers from the cybersecurity industry to the North Dakota State University to give National Cybersecurity Career Awareness Week presentations. The presentations had three parts. In the first part, the speakers gave their presentation which was recorded and archived (for four of the five speakers, one was not able to have his presentation recorded) on the NDSU Institute for Cyber Security Education and Research website. In the second part, the speakers took questions from the audience which were also recorded as part of the presentation. Finally, in the third part, they held a more informal and intimate question and answer session with the students who were able to get feedback on their personal potential for success in different career paths within the cybersecurity industry and on their resumes.

Because all of the presentations are archived, students are able to view them at any time. We're also able to embed relevant content from the presentations into class lectures and other appropriate places. Over time, we hope to build up a library of numerous presentations covering a wide variety of areas of cybersecurity career opportunities.

Watch the presentations at https://www.ndsu.edu/cybersecurity/speakers/

BENEFITS

The event was a big success and the format we chose allowed us to have a public portion (that we recorded) and more informal and intimate portion where students were able to get specific personal feedback. Students and speakers stayed at these events long after their scheduled ending time, demonstrating how high the interest was on both sides. Several students have pursued internships and jobs based on the conversations started at this event. By recording the presentations, we've created the beginnings of a library that can be accessed by our students as well as students at other institutions. We plan to continue to add to this library with presentation recordings from future years National Cybersecurity Career Awareness Week presentations.

CONTACT INFORMATION

Jeremy Straub
jeremy.straub@ndsu.edu
(701) 231-8196
North Dakota State University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

PROVIDING STUDENTS HANDS-ON EXPERIENCES AND VOLUNTEERISM THROUGH COMMUNITY

LOCAL PARTNERSHIP

DESCRIPTION

Most Cybersecurity and Computer Science positions require experience, While going to school in a rural area, finding a job in the Computer Science and Cybersecurity field is difficult. This often causes stress for students who are unable or willing to relocate for employment, but wish to enter the Cybersecurity or Computer Science disciplines. Faculty started working with local business to create internship, mentoring, and shadowing opportunities for Cybersecurity, IST, Computer Science students. Students are empowered to solve problems, troubleshoot, research, consult other professionals, and complete real-world task putting their classroom knowledge to the test. Professors often have difficulty developing authentic learning opportunities, that are unique, and timely given the limits of time, budget, and equipment. Partnering with local businesses solves the problem with only a negligible impact on resources. It benefits faculty as they stay connected to the community. It benefits students as they get to experience situations and work with different equipment and settings. Students who take part in the internships get to graduate with experience and professional references.

Recently on a webinar with the Department of Homeland Security they talked about the importance of students participating in CTF competitions on the Cybersecurity side and Code-a-thons on the Computer Science side. These competitions give students an opportunity to test their skills but more importantly practice their soft skills like communications, team work, out-of-the-box/creative think, and planning. It also gives students who participate in employer/vendor sponsored competitions an idea as to the skills that employer is looking for. While work experience through internships is important, just like skill building and validation is important through competition, volunteerism is the third side of the learning triangle. Computer Science, Cybersecurity, and IST students are provided opportunities and encouraged to volunteer their time at community events for non-profits like Girl Scouts to teach them about technology. Student volunteer for two hour shifts for a two-day event that lets them talk with approximately 3000 seventh graders about technology and why it is a field they should continue. This helps students explain their skill set to a non-technical person, something they will all do in their professional career.

BENEFITS

Students work on soft skills as well as technical skills. They are building their professional network and obtaining professional references. They are instilled with a sense of community and volunteerism to make the world a better place. They get to see first hand how the concepts learned in the classroom are applied in the real-world and they gain an understanding that they have so much more to learn and they cannot learn everything from textbooks and professors. This triangle learning approach can serve as a model for high schools, trade schools, 2-year and 4-year institutions.

CONTACT INFORMATION

Melissa Stange & Henry Coffman
mstange@lfcc.edu
(540) 868-7000
Lord Fairfax Community College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

SETTING UP AN ADVISORY BOARD AND PARTNERSHIPS THAT WILL HELP GUIDE AND GROW YOUR PROGRAM

LOCAL PARTNERSHIP

DESCRIPTION

Bossier Parish Community College (BPCC) Cyber Technology program was built from the ground up by faculty that saw the need for cyber security. Since we started just over ten years ago we have grown to 250+ students in our program. In addition BPCC is recognized by the state of Louisiana as a Center of Academic Excellence in Information Assurance. The campus is located right beside the Cyber Innovation Center and the CSRA's Integrated Technology Center (ITC) as well as easy distance of multiple other venues that enable us to have a strong advisory board to help steer our programs to better enable us to train the work force of tomorrow.

It is felt that a strong connection to the local IT industry is a MUST. This connection is what enables us to stay on top of trends and demands in our area and be sure that our students are work force ready upon leaving our program. We have learned you cannot custom make a course for just one industry, but must find a way to find a blending that will serve multiple partners at the same time. Working with an advisory board in a round table situation has enabled our partners to learn from each other and gain insight that will benefit everyone.

BENEFITS

We have worked hard to grow our advisory board and connection with local industry. We strongly feel that adds value to our program as it works to ensure that our programs are adding value to the local work force. In addition we are able to provide focused certification and training for our local companies.

CONTACT INFORMATION

Chris Rondeau
CRondeau@bpcc.edu
(318) 678-6317
Bossier Parish Community College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

STUDENT & FACULTY LIBRARY PRESENTATIONS

LOCAL PARTNERSHIP

DESCRIPTION

The North Dakota State University Institute for Cyber Security Education and Research launched a series of library presentations at libraries around the state in the 2017-2018 academic year. As part of North Dakota's land grant institution, we wanted to reach out to the public in the same way that the NDSU extension offices reach out to those in agriculture and related fields.

Students and faculty went to several different libraries in different parts of the state and gave a prepared presentation and answered questions from the audience. These questions ranged from relating to personal information protection practices to business best practices to asking questions about educational opportunities. The presenters also brought a variety of printed materials that were made available to the attendees to take and read. The ages attending the presentations varied widely as did the background of the attendees.

In addition to providing an excellent resource for North Dakota residents, the program allowed students to gain public speaking experience and really helped them to understand how much more they know (i.e., have learned) as opposed to members of the general public. Students also learned about cybersecurity topics as they were preparing their presentations.

BENEFITS

The library outreach program had a number of benefits. First, it is well-aligned with NDSU's land grant mission and provides a model for other land grant institutions in this domain. Second, the program provided valuable information to members of the public in different areas of the state. Third, for some that may have a negative impression of youth, generally, and university students in particular, these presentations allowed them to see the students in a very positive light. Finally, the presentations provided an excellent opportunity for student learning (in their preparation) and to gain and demonstrate their presentation skills. The presentations were also seen as resume builder items by some students.

CONTACT INFORMATION

Jeremy Straub
jeremy.straub@ndsu.edu
(701) 231-8196
North Dakota State University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

THREE COLLEGES + THREE DEGREES = ONE SUCCESSFUL CYBER CAREER

LOCAL PARTNERSHIP

DESCRIPTION

Through the leadership of our provost, Dr. Debbie Ricker, Hood recently established a formal pipeline with two nearby colleges in Frederick County—Frederick Community College (FCC) and Mount Saint Mary's University (MSMU)—to provide students in the region with opportunities to obtain cybersecurity training at every level of higher education (associate's, baccalaureate, and master's).

Students who graduate with an Associate of Applied Science degree in cybersecurity from FCC and complete certain academic requirements can transfer up to 60 credits to MSMU, with a maximum of 24 credits meeting MSMU's cybersecurity major requirement. There are two options for degree articulation between Hood and MSMU: (1) the 4+2 Program that grants qualified MSMU students preferred admission into the cybersecurity M.S. program at Hood and (2) the 3+2 Program, an accelerated track that will allow qualified MSMU students to earn both a B.S. in cybersecurity from MSMU and M.S. in cybersecurity from Hood in only five years, one year less than the typical time. MSMU students accepted to either program will be able to take courses at Hood that will count toward their B.S. degrees and have the opportunity to waive foundational courses upon entry into Hood's M.S. program.

In an effort to support the growing need for trained professionals in the cybersecurity field, both regionally and nationally, the three colleges have collaborated to provide a single, unified degree pathway into this field. All three cybersecurity degrees—associate's (FCC), baccalaureate (MSMU), and master's (Hood)—will be marketed together to encourage all students in the region to pursue advanced cybersecurity training. All three institutions will promote these programs, hoping to attract qualified students and streamline their path to pursuing higher education and succeeding in the cyber field.

BENEFITS

There are a variety of benefits from this three-way partnership:

1) Tuition and time savings for the students
2) Unique learning opportunities for students by seamless sharing of computer lab facilities and software
3) Unique cross-mentorship opportunities for students with faculty from multiple institutions
4) Unique faculty collaboration opportunities to improve pedagogy and engage in research projects and scholarly activity
5) Unique student networking opportunities with cyber teams practicing and participating in hackathons and other cybersecurity related events
6) Shared marketing opportunities for program exposure and student recruiting across three institutions.

CONTACT INFORMATION

April Boulton
boulton@hood.edu
(610) 209-5012
Hood College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

05

STUDENT LEARNING AID

WINNING SUBMISSION:

COMIC-BEE: BRANCHING, INTERACTIVE WEB COMICS FOR CYBERSECURITY EDUCATION AND ASSESSMENT FOR LEARNERS OF ALL AGES AND LEVELS

COMIC-BEE: BRANCHING, INTERACTIVE WEB COMICS FOR CYBERSECURITY EDUCATION AND ASSESSMENT FOR LEARNERS OF ALL AGES AND LEVELS

STUDENT LEARNING AID

DESCRIPTION

Comic-BEE helps educators and evaluators at all levels rapidly create web comic stories that convey valuable lessons in cyber security, without need for artists, writers, or programmers. Developed with input from instructional design educators and based on research funded by the Department of Homeland Security Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD), Comic-BEE simplifies and accelerates the creation and delivery of these interactive, educational materials through a unique system that enables authors to easily develop branching storylines using advanced automation technologies and pre-rendered art assets. Students can achieve a deeper understanding of cyber concepts by creating their own comic that show how situations unfold with different positive and negative outcomes. In addition, Comic-BEE's scoring capability supports evaluation and assessment of diverse cyber concepts and skills by using branching web comics for hands-on evaluations, or practice exercises and labs for process and strategy. Through several local partnerships, we have piloted and demonstrated Comic-BEE (https://www.comic-bee.com) in a variety of educational settings. A graduate student at a local university created a series of comics to be used as part of undergraduate classroom curriculum on ethics. Students at several summer cyber camps used Comic-BEE to create comics on security awareness topics. College students have used Comic-BEE to create branching web comics as a capstone activity to demonstrate what they learned in a course, rather than writing a traditional term paper – an option popular with both students and instructors. Competitors in the National Collegiate Cyber Defense Competition used Comic-BEE to create web comic stories to educate the employees in the fictional companies they defended during the competition. And with funding from the National Science Foundation, we are conducting a series of workshops for middle school students in which the students read web comics on cyber topics, and then use Comic-BEE to create their own story about a cyber crime investigation (http://www.ic.sunysb.edu/Projects/bigsce/about.html).

BENEFITS

Developing interactive, graphic stories the traditional way is costly and time-consuming and requires specialized skills that present barriers to creation and dissemination of the interactive curriculum. With Comic-BEE, you can create a full, interactive web comic in days, not weeks. This approach provides low-cost development of interactive curriculum and evaluation materials – with no licensing fees for digital content. As a web application, there's no software to install or maintain, all you need is an HTML 5 compliant browser to create or read web comics. Comic-BEE makes it easy to share the web comic curricular materials with other educators, and it is simple to change a comic configured for exploratory learning to a scored comic for assessment. The "point and click" web user interface allows you to rapidly refresh or customize a comic for a different target audience: modify the comic content to suit the expertise, age, environment or demographics of your audience. The built-in scoring capability means comic readers can practice and refresh their skills or demonstrate their cyber competence in a cyber competition with no formal setting or computer lab required.

CONTACT INFORMATION

Laurin Buchanan
laurin.buchanan@securedecisions.com
(631) 759-3926
Secure Decisions

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

ANGEL-TECHS SUPPORT GROUP

STUDENT LEARNING AID

DESCRIPTION

Angel-Techs assists Non-for Profit organizations with their computer systems needs. They are in charge of projects that would benefit these organizations who lack the funds and IT expertise to hire a Computer Professional.

Other tasks involve helping other Departments at Westchester Community College with special projects and research for Computer solutions. The Angel-Techs students assist honor students with new software and hardware acceleration projects, students in need who could not afford a pc by loaning equipment and supporting it and helping new students in the first week of school with questions and issues related to their Blackboard shell access and software apps requirements loaded in their computer.

The program is growing very fast and students who participated in the past were able to leverage very successfully this applied experience at job interviews.

BENEFITS

Students are in a difficult situation when searching for a computer job. Without hands-on experience, students are finding that quality companies are turning them down for candidates with more IT experience. Angel-Techs gives them this valuable hands-on experience. In the past, companies used internships as a way to train possible employees and gain some less costly labor. Today, many companies do not have the resources to train employees to a specific position. Angel-Techs acts like an internal internship, training students in a variety of IT endeavors. This is an innovative solution to this problem by using the Cybersecurity students who have a more vast knowledge and are able to leverage their broader understanding of Information Technology to help others.

CONTACT INFORMATION

John Watkins
John.Watkins@sunywcc.edu
(914) 606-8519
Westchester Community College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

CYBER EXPLORATIONS: DESIGN, PROVISIONING AND MANAGEMENT OF A 24/7 ONLINE ALL-THE-TIME SCALABLE NETWORK OF STUDENT SUBNETS - EACH CONTAINING ONE OR MORE VIRTUAL MACHINES BEHIND A STUDENT MANAGED FIREWALL IDS/IPS

STUDENT LEARNING AID

DESCRIPTION

A flexible design was created to allow each of the students in a lab environment (physically or online) to access an individual Virtual Student Subnet. Each Virtual Subnet would contain one or more Virtual Machines (Windows and/or *nix) behind a Virtual Student Managed Firewall IDS/IPS.

The provisioning of the Virtual Student Subnets is accomplished through an Application developed to utilize the Microsoft Hyper-V environment. Provisioning is done by first creating up to 9 different configurations consisting of primary boot VHDs and optional secondary VHD devices. Provisioning is then executed by selecting a configuration to be applied to individual students or groups of up to 250 students - each having their own subnet consisting of an individual Firewall IDS/IPS and VMs - all student accessible.

The design and provisioning is maintained on a scalable hardware platform which can be portable or rack-based systems. The platform is also designed to provide students access to their subnets and VM's on a 24/7 online all-the-time basis through an HTML5 Browser Interface coupled with Cybersecurity and Cyber Forensics exercises developed at Embry-Riddle Aeronautical University.

BENEFITS

The CyberExplorations solution implemented at Embry-Riddle Aeronautical University provides a low cost of entry, highly scalable, easily maintained solution for providing Cybersecurity and Cyber Forensics training. The solution is ideal for classroom labs, online labs and portable labs (i.e. Computer summer camps). The solution also allows for student VMs to be left running 24/7. This allows students to terminate their access to a VM and re-access it later, right where they left off (unless its a Windows VM and it is the second, and sometimes fourth, Tuesday of the month). But perhaps the biggest benefit of all is the uptick in student and faculty engagement and satisfaction, demonstrated in unsolicited comments when the solution was first implemented.

CONTACT INFORMATION

Glenn Dardick
gdardick@dardick.net
(804) 402-9239
Embry-Riddle Aeronautical University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

CYBER TWEEN

STUDENT LEARNING AID

DESCRIPTION

This dual-enrolled Lord Fairfax Community College student wanted to help Tweens, students in middle school, be more cyber aware how they are participating in voluntary and non-voluntary harmful activities in our technology driven society. Middle School educators are engaging students with use of more technology and often they do not think about the possible cyber criminals larking on these "free sites". Parents are creating accounts for their Tweens who do not meet the minimum social media account age limits. With the world of online sharing, people often do not know about meta data associated to photos and how it can identify them and locations to cyber criminals. To address these issues the student designed and held a Cyber Tween event in which different types of Cyber Specialist spoke with the participant. Topics covered were identity theft, Meta Data, Cyber Stalking, Security Controls, Passwords, Social Media, Cybersuicide, Phishing, Sexting, Malware, and Ciphers. Resources were provided for home use and a website was create (http://www.rachels.online/cyber-awareness/) so participants could continue learning after the event. The second portion innovation involved helping educators learn what cybersecurity is and how they can keep their students safe online. Educator training was done through quarterly professional development (teacher work day) presentations. The NSA Day of Cyber was completed at both the Cyber Tween and Educator Workshops. The third part of this innovation is to arrange Cyber speakers in local schools to continue keeping Cyber Awareness at the fore front of Tweens minds. The final part of this innovation was parent education. Resources were provided to parents about a local girl stalked online, abducted, and what she learned and hopes to tell others so it does not happen to them.

BENEFITS

The benefits of the innovation is that local Tweens through in person presentations, local middle school educators, and Tweens globally through the website can learn about how to get help if they are considering Cybersuicide or are being Cyber Bullied and how to keep their personal information personal. As more K12 schools start to teach introduction to cybersecurity, educators will have some foundational knowledge and resources. Educators will be more cautions about requiring students to create accounts blindly on "free" online sites. Parents are aware of why they should not create accounts on social media before age limit is reached, why sharing photos of child's life online is not smart, and how to keep private information save. This innovation can serve as a model for other students to do in their local areas to educate on Cyber Awareness. Making people more informed may also increase the interest in the Cyber profession, which will increase enrollment in Cybersecurity academic programs.

CONTACT INFORMATION

Rachel Stange
ms25145@email.vccs.edu
(540) 877-5571
Lord Fairfax Community College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

CYBERSECURITY CAREER GUIDE

STUDENT LEARNING AID

DESCRIPTION

Our Cybersecurity Career Guide is a great resource for middle school and high school students. Our 52-page magazine-style guide includes:

- An explanation of cybersecurity: From malware and phishing to ransomware and password attacks, how these cybercrimes affect every industry.
- Types of cyber jobs: Roles in cybersecurity as defined by the National Initiative for Cybersecurity Education (NICE), along with salary information.
- Education pathways: High school prep—all about classes and competitions, where to go for associates degrees and certificates in cybersecurity, four-year colleges and universities that specialize in cybersecurity
- Support for women and minorities
- Careers in nearly every industry: Private-sector companies that hire cybersecurity professionals, firms that specialize in cybersecurity and government cybersecurity careers

BENEFITS

This publication allows middle school and high school students can clearly see the various pathways to a cybersecurity career, whether it be starting with a cyber certificate, going to a community college for an Associate's degree, or attending a four-year college—or all three! It is packed with valuable information on the types of classes to take in high school, cybersecurity competitions, schools offering the various degrees, the types of careers available, internship opportunities, scholarship information, and salaries offered at different career levels.

CONTACT INFORMATION

Stacie Harrison
sharrison@start-engineering.com
(202) 302-1989
Start Engineering

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

CYBERSECURITY EXPERIENTIAL CYCLE OF PROFESSIONAL EXPERTISE (CECPE) PROCESS

STUDENT LEARNING AID

DESCRIPTION

Success as a cybersecurity professional is determined far more by someone's ability to do things rather than someone's ability to know things. As students go through this experiential cycle, they discover what they enjoy and what they are good at.
Cybersecurity Experiential Cycle of Professional Expertise (CECPE) Process

The seven sequential stages of the CECPE learning cycle continuously strengthen the professional expertise and execution skills of cybersecurity professionals, students and digital forensics examiners in our graduate programs. The process is open and welcomes graduate students from all backgrounds and has successfully allowed high levels of gender and racial inclusion and diversity of ideas into the profession, while removing artificial entry barriers.

Foundational Principles Each stage in the CECPE learning cycle is supported by a foundational principle of professional expertise:

1. We all do many things in life that help us develop a wide range of skills
2. As we develop skills, new doors of opportunity open up for us to use those skills
3. As the doors open, we begin to find ourselves
4. In each new opportunity, we get closer to finding ourselves
5. We get closer to learning the things we are good at
6. We get closer to discovering our passion and what we truly enjoy
7. As we pursue our passion and enjoy our lives, we complete the Cybersecurity Experiential Cycle of Professional Expertise cycle only to resume the cycle once again to take our careers to the next higher level

BENEFITS

Embracing this perennial process is the foundation for a dynamic and rewarding career as a cybersecurity professional. After completing the Cybersecurity Experiential Cycle of Professional Expertise, students are professionally poised, well-trained and strongly equipped to begin a new experiential professional cycle of excellence in the cybersecurity field. This powerful process of experiential self-discovery and conscious sorting, monitoring, collaborating, and applying continually higher levels of knowledge perpetually is the foundation of the competency-based cybersecurity teaching model at UMUC.

CONTACT INFORMATION

Patrick O'Guinn, Sr.
patrick.oguinn@umuc.edu
(240) 684-2071
University of Maryland University College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

DEVELOPING AN AI ENABLED LEARNING ASSISTANT & KNOWLEDGE ANALYTICS PLATFORM FOR ACCELERATING SHARING KNOWLEDGE, SUSTAINING ENGAGEMENT AND ENHANCING CAREER SKILLS TRAINING, LEARNING AND TEACHING CYBERSECURITY AWARENESS, CERTIFICATION TEST PREPARATION AND COMPLIANCE FOR DIVERSE POPULATION & LEARNERS..

STUDENT LEARNING AID

DESCRIPTION

Current career training options are not as accessible, efficient or cost effective as they can be. We propose the use of AI, Semantic Knowledge Graphing, Conversational digital assistant mentor and knowledge data mining to deliver a new generation of student learning aids, lab activity, interlinked and aggregated curriculum, job skills and job seeker engagement and career promotion. Given a whole new set of enabling analytics and assistive technologies, and our experience and expertise, we have been working on minimum viable product version of this platform and piloting it in our local cyber security workforce development collaborative initiative.

We have noticed through pilots, experience and observations that if we increase and scale the level of engagement of learners and trainers communications, conversations, connection to real life teaching moments, demonstrating practical professional problem solving scenarios, incorporating variety of learning resources, addressing learning inquiry as soon as it occurs, regardless of time, place, and career objective we can increase the skills development, continuous learning and application of learning in real life problem solving. We acknowledge the fractured experience of cyber security career enthusiasts having to piece together variety of news on causes of cyber safety and data privacy breaches, and their correlation to core cyber security standard frameworks, risk management compliance, learning resources, pathways, career coaching and preparing for hands on projects and job opportunity options.
We would like to enhance the learning experience and scale the capacity and competency of the trainer during the cybersecurity training. We can bridge the gap between conceptual content, relevant and engaging lab and learning practice activities and great variety of learnign resources and hands on project available locally or on line.

BENEFITS

1. Increase the learning outcome- increase learners focus, sustain and deepen their engagement in learning process - because they can access their Digital learning mentor 24 X& any time any where, at a pace they don't get overwhemed, via their internet connected device (initially via mobile or web based applications). Learner can ask questions, receive relevant response related to the syllabus and stated learning objectives and practice in preparation for compliance testing.
2. Assist the trainer to scale, address high volumes of posts and inquiries from learners.
3. Increase opportunity for knowledge & experience transfer between learners, trainers and mentors; with every iteration, track activities, and analyze results , drive insights to enhance curriculum, training practice based on the learning, inquiring and responses related to cyber security standard framework, learning framework and career options.

CONTACT INFORMATION

Abby Ameri
operations@exxoteck.com
(925) 963-5434
A collaboration between Exxoteck Inc and local colleges
(San Jose City College, Arizona State University)

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

HOW TO GET STUDENTS EXCITED AND INTERESTED IN CYBERSECURITY AND ETHICAL HACKING WHEN THEY DON'T KNOW WHAT IT IS?

STUDENT LEARNING AID

DESCRIPTION

How do you explain ethical hacking and cybersecurity to students to get then interested in a career in cybersecurity? Show them. Local arcades have games of skill most of our students have played and lost. What if we could show them how to build a device which would allow them to be a winner every time they played?

With inspiration from an engineer who worked on the Curiosity rover my students and I built a replica of a popular arcade game. To teach them about cybersecurity they were shown how he game's programing could be modified so they could be a winner every time they played the game.

To teach them how the game could be hacked my students built a device which gave them a mechanical advantage, so they could win every time.

BENEFITS

In having my my students build a game and a device which allowed them to win the game every time they had to work together as a team and use critical thinking skills in design and functionality. By having students build and program the game and the device which allowed them to win every time they could easily explain cybersecurity and hacking to other students in away they could instantly understand.

CONTACT INFORMATION

Doug Spindler
dspindler@marin.edu
(925) 258-6600
College of Marin

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

PARTNERSHIP WITH UNITED STATES MARINE CORPS OFFICERS

STUDENT LEARNING AID

DESCRIPTION

Cybersecurity can have most of the elements of a Hollywood blockbuster (and has been, of course, the subject of several top movies). However, most people don't get to see it from this exciting perspective. To engage our students at the North Dakota State University, we invited former cyber operator and Marine Corps Major Terry Traylor to help teach our Ethical Hacking course. In addition to presenting technical content, Terry was able to engage the students with his personal prior involvement with 'in the trenches' cyber and information warfare.

Traylor, who volunteered, was aided by Asst. Prof. Jeremy Straub who was responsible for the course overall, systems administrator Guy Hokanson and undergraduate systems administration assistant Demitrius Fenton. To support the effort, Fenton created numerous virtual lab environments that students could safely practice their hacking skills within. The course also used a flipped classroom methodology, allowing it to support any emergencies or schedule requirements of Maj. Traylor, as well as enabling re-use of the lecture content in future years. The format for the e-learning approach was designed by Straub and will be used in other NDSU cybersecurity courses, including one currently in progress and several under development. Classroom time was able to be devoted to answering student questions, aiding them with their lab exercises and other high-interaction activities. Students took practice tests in our online learning environment which were patterned after EC Council's Certified Ethical Hacker examination and received feedback on their performance to aid them in preparing for the real examination. The partnership with Maj. Traylor also yielded benefits from his network of contacts who were able to aid in other areas of course development, including providing support for lab exercise development. Students got a 'best of both worlds' experience with Traylor providing real-world content and Straub covering theory, ethical and legal topics.

BENEFITS

The partnership resulted in very high levels of student engagement. Tying instructional objectives to the EC Council Certified Ethical Hacker exam made it unambiguous to students why each area of content was important. Students were aware of the value of this certification to them and went the extra mile to learn in order to be able to achieve it. In addition, the approach taken to the course, including the use of video-recorded lectures, electronic testing and deployable lab exercises facilitates offering the course in future years. Most of the content can be reused (with incremental enhancement and modification), providing students a superior learning experience while allowing us to focus our efforts on developing additional cybersecurity courses. In particular, efforts on this course can focus on areas where students indicated that additional practice was needed or where they were confused, allowing maximum benefit from the time devoted to these activities.

CONTACT INFORMATION

Jeremy Straub
jeremy.straub@ndsu.edu
(701) 231-8196
North Dakota State University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

STUDENT COURSE CO-DEVELOPERS

STUDENT LEARNING AID

DESCRIPTION

Cybersecurity concepts can be challenging for students who must learn new terminology, the attack-defense paradigm and tool names while also trying to understand the core material. This can be even more complex for specialized topics, such as covering legal topics. To aid students in their understanding, we wanted to make sure that we were presenting the material in the most accessible format possible. To this end, we employed several undergraduate students as course co-developers. These students took materials selected or created) by the faculty course developer and reviewed them to see if they understood them. They then asked any questions and we collaboratively corrected any issues with or deficiencies in the materials. The students then re-presented them in the way that they would, if they were explaining the topic to a fellow student.

The output of this became the basis for the course lectures. Specifically, this content was used for lecture slides and influenced the oral presentation of the topic by the faculty instructor. In addition, the students were recorded providing demos and other content which were inserted into the lectures at appropriate points. This made these areas very accessible, as someone their own age was demonstrating the techniques. This video content can be used for both in-person and flipped classroom (recorded lecture video) course formats.

The students who helped develop these courses gained significant educational value (in addition to getting paid for the development work) from their immersion in the material and the deeper understanding that they had to gain of it to present it to their peers.

BENEFITS

The use of student course co-developers provided benefits in a number of areas. It made the courses more accessible and, through this, more interesting to students by removing points of confusion that could come from language or concepts that they were not familiar with. The approach also maximizes the use of faculty time, facilitating the development of additional course materials and exercises, by allowing students to perform work that they are as well or better suited to perform. The student demonstration content adds significantly to the course and would not have been feasible, time-wise, to be setup and performed by a faculty member. Finally, there was tremendous benefit to the student course developers. They gained a far more deep and detailed understanding of the material that they would have by just taking the course. Several also have expressed an interest in pursuing graduate degrees and teaching careers after this experience.

CONTACT INFORMATION

Jeremy Straub
jeremy.straub@ndsu.edu
(701) 231-8196
North Dakota State University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

THE CYBER SECURITY SPOOKHOUSE

STUDENT LEARNING AID

DESCRIPTION

Each October, in recognition of Cyber Security Awareness month, the Cyber Security and Forensics students at Tulsa Technology Center produce a Cyber Security Spookhouse (Spookhouse). The purpose of Spookhouse is to raise awareness of cyber security issues for a general audience and to recruit future students. At its core, Spookhouse is a cyber security awareness project related to the personal use of technology. All students are encouraged to suggest topics for Spookhouse and develop concept proposals to present to the instructors. Based on class size and space availability, Spookhouse generally presents eight topics. Once the topics are selected, students submit their ranked preference for topic assignments. The eight selected topics become the eight booths of Spookhouse. Past booth topics have included such diverse areas as Wi-Fi security, Bluetooth security, USB security, IoT security, automotive and aircraft networks, and identity theft.

Each booth team is charged with developing deliverables for its booth. Those deliverables include a topic specific brochure to be distributed to booth visitors, posters, decorations (spook house theme), presentation talking points, and a demonstration. Demonstrations can be simple simulations or complex displays of technology, depending on the ambition of the team members. One Spookhouse booth, in order to demonstrate the insecurity of wireless automotive key fobs, borrowed a car from the Tulsa Tech automotive class and proved that a software defined radio could intercept and replicate unlock codes. Generally, students are given one week (15 class hours) to develop deliverables, set up and decorate Spookhouse and rehearse their talking points and demonstrations.

BENEFITS

The Spookhouse achieves a number of desirable outcomes. First and foremost, it affords students the opportunity to teach others about technical cyber security topics. Teaching these topics ensures that students will retain that information long after they would have forgotten it had they only received it in lecture or by reading. Second, it gives students a simulated trade show experience preparing them for an aspect of an IT career that most IT professionals have to learn "under fire." Learning to collaborate and coordinate booth presentations without face-to-face contact provides students with the experience of teamwork in multi-site enterprises. Visitors are made aware of cyber security risks in an environment intended to induce fear (mildly). Based on visitor comments, this seems to help with their retention of the topic materials. Additionally, visitors are made aware that their bad habits can produce far reaching negative results.

CONTACT INFORMATION

Jens Mache
jmache@lclark.edu
(503) 768-7564
Lewis & Clark College

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

THIS WEEK IN CYBERSECURITY

STUDENT LEARNING AID

DESCRIPTION

This is a simple, yet quite effective teaching method I introduced to both undergraduate and graduate courses. At the beginning of each class, we start with "This Week in Cybersecurity" reviews. Each student brings in something related to cybersecurity that has been breaking news, research, academic publications, etc., from the last calendar week. The purpose is two-fold. First, to continuously reinforce to students the fact that the science and operations of cybersecurity changes as such a breakneck pace that there is a plethora of new and important information in such a short timeframe as one week. And second, to bring forward relevant and timely technical, legal, social, and security related issues to discuss and apply to the course objectives. The students embrace this assignment with gusto and often compete to find the most interesting, complex, and applicable topic.

BENEFITS

The benefits are that the students a) stay current with cybersecurity changes, vulnerabilities, issues, opportunities and topical issues and b) are able to grasp the impact of the threat by conducting a weekly mini-research project to seek and find a topic to discuss in the "This Week in Cybersecurity" forum.

CONTACT INFORMATION

James Curtis
jamescurtis89@webster.edu
(314) 246-8761
Webster University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

USE OF STATE-OF-THE ART RESOURCES OF GLOBAL INDUSTRY CONSORTIA FOR CYBERSECURITY LEARNING AND RESEARCH

STUDENT LEARNING AID

DESCRIPTION

The importance of Cybersecurity education in colleges is increasing continuously. Recently the demand of qualified graduates in Cybersecurity is strong as Cybersecurity industry requirements are becoming more diverse and complex compared with the past.

To satisfy this strong demand from Cybersecurity industry, Cybersecurity education at the college should be aligned to accommodate more "up-to-date" and "emerging" security and related technologies that the students can use them in their jobs right after graduation as a kind of preemptive education.

I propose to use TM Forum (https://www.tmforum.org/) which is the global industry association that drives collaboration and collective problem-solving to maximize the business success of communication and digital service providers and their ecosystem of suppliers. I have been using those resources in my Cybersecurity courses teaching since the year of 2011. Especially, TM Forum's resources of the group called Security, Privacy & Trust (https://www.tmforum.org/security-privacy-trust/) can be used for the student's research in figuring out the state of the art of Cybersecurity industry readily before their graduation from the colleges. Another one is LoRa Alliance (https://www.lora-alliance.org/) which is an open, non-profit organization dedicated to promoting the interoperability and standardization of low-power wide area network (LPWAN) technologies to drive implementation of the Internet of Things (IoT) that security component is very crucial. Regent University became the first university member of LoRa Alliance in America in March 2017.

BENEFITS

The following benefits can be expected:

1. The opportunities to perform practical research projects relevant to Cybersecurity courses can be given to the students.
2. The latest industry documents of an international telecommunications consortia TMForum and LoRa Alliance can be accessed for Cybersecurity courses research activities by the students.
3. The students can practice of acquiring faster and accurate "live industry documents" for their research.
4. The students can practice to increase their critical thinking capability through their industry oriented research activities.
5. Students can get an opportunity to figure out the relationship between the content of a course and Cybersecurity research work they are performing.

CONTACT INFORMATION

Young Choi
ychoi@regent.edu
(757) 352-4949
Regent University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

USING HAK5 PRODUCTS TO INCREASE CYBERSECURITY PENTEST AWARENESS FOR SECURITY ASSESSMENT AND AUDITING

STUDENT LEARNING AID

DESCRIPTION

Texas State Technical College utilized bleeding edge security applications, products and hardware to increase the reach of students ability to grasp understand and comprehend the concepts behind penetration testing. By utilizing Hak5 products like: Packet Squirrel, LAN Turtle, Wifi Pineapple, Bash Bunny and USB Rubber Ducky students are able to take these products and test them in a 'real life' scenario. Where they can attempt to invade/intrude in an isolated environment. Students are tasked in learning each device, how it is implemented and how to infiltrate into the isolated ADDS, CISCO network environment.

BENEFITS

Once the products are learned it's time to prevent future attacks. Students are tasked to block or prevent future intrusions. Students in ITSY-2359 Security Assessment and Auditing perform audits during and after the attacks take place. Students learn different techniques and methodologies for hardening network, operating systems and environments that makes them valuable assets to any company. As any student that has taken the course they say best part of this is they get to be a real life "Penetration Tester" or "Grey Hat Hacker" and learn the vulnerabilities of what can happen if you don't take Information Technology Security seriously.

CONTACT INFORMATION

Ryan Hill
rahill@tstc.edu
(346) 239-3449
Texas State Technical College Fort Bend

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

USING KALI LINUX TO PERFORM REAL LIFE PENETRATION

STUDENT LEARNING AID

DESCRIPTION

Kali Linux is a great operating system that teaches how versatile Linux and it's packages are. Students learn how to install/configure Kali in a secure environment then attack Metasploitable2 and Windows Operating Systems XP, 7, 8 and 10 using known CVEs. Learning how attackers can infiltrate Operating Systems through various means students are then able to take that knowledge and apply systems to detect and even block these types of attacks from occurring through IDS/IPS systems. For course ITSY-2330 Intrusion Detection being able to invade systems is a critical skill that students can then take to the job market and add to their resume.

BENEFITS

Aside from learning these Kali hacking skills, students then learn the different methodologies and practices needed to secure environments and then how to protect those environments. By preventing these types of attacks students are able to add this to an ever growing skill set they have hands on training in. This type of hand on labs and training provides TSTC students the necessary resume building skills needed to excel in the given career of their choice.

CONTACT INFORMATION

Ryan Hill
rahill@tstc.edu
(346) 239-3449
Texas State Technical College Fort Bend

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

VIRTUAL MACHINE CYBER RANGE

STUDENT LEARNING AID

DESCRIPTION

To facilitate student learning, particularly in our ethical hacking course and other cybersecurity courses, we developed a virtual machine-based cyber range. The virtual servers house multiple virtual machines which are interconnected using virtual switches and routers. A complete and isolated virtual environment can be created for each student. These virtual environments can be replicated and reset to facilitate repeated use in a course environment. The virtual machines can be accessed through an interface that allows remote control, without connecting the virtual machines operating system to a public or private network directly and risking their intentional or inadvertent attack against it.

The virtual range is protected by a firewall unit that acts as a second layer of protection. It scans and filters traffic, allowing only traffic for the remote connection interface through. Thus, if the virtualization software itself was compromised in some way (by student/user activity or otherwise), the firewall would still offer the public and local private network protection.

Lab exercises were created by Demitrius Fenton and Terry Traylor, using the cyber range, to support our ethical hacking course. These exercises allow students to get hands-on experience attacking actual systems, running a variety of operating systems, in a controlled and safe environment. In these exercises, the students will be given one or more workstation virtual machines to start from. They can be provided information about the status of their scenario network or be required to scan and ascertain its configuration on their own (as would be required when attacking an unknown network). Students can be required to capture information 'flags' to demonstrate scenario completion or the end state of the scenario network and virtual machines can be assessed.

BENEFITS

The virtual machine cyber range provides a number of benefits. The use of virtualization makes the entire thing feasible and scalable, removing the need to build out hardware infrastructure for each student in a course. The remote access mechanism allows the cyber range's use by distance students and provides convenience of access for on-campus students. The cyber range allows students to gain hands-on experience with hacking techniques and other cybersecurity concepts, preparing them to 'hit the ground running' when entering a relevant internship or entry-level position. We compared building the system ourselves (with vendor and military volunteer aid) to the use of pre-existing online cybersecurity laboratory solutions. Building the system ourselves provided significantly more flexibility in terms of customizing labs to instructional goals (instead of using fixed, vendor-developed labs) and flexibility to change and adapt quickly in the future. It also removed the significant per-student cost required for the use of vendor-supplied online labs.

CONTACT INFORMATION

Jeremy Straub
jeremy.straub@ndsu.edu
(701) 231-8196
North Dakota State University

TRANSFERABLE

Yes, this innovation is transferable to other institutions.

NATIONAL
CYBERWATCH
CENTER

WWW.NATIONALCYBERWATCH.ORG