Academic Papers

Academic Influence of Social Network Sites on the Collegiate Performance of Technical College Students

Jameson McFarlane, Thorne Jameson McFarlane, Leon Bernard

Paper of the Year

Social network sites (SNS) is an emerging phenomenon that is here to stay. The popularity and the ubiquity of the SNS technology is undeniable. Because most SNS are free and easy to use people from all walks of life and from almost any age are attracted to that technology. College age students are by far the largest segment of the population using SNS. Since most SNS have been adapted for mobile devices, not only do you find students using this technology in their study, while working on labs or on projects, a substantial number of students have been found to use SNS even while listening to lecture. This study found that SNS use has a significant negative impact on the grade point average of college students particularly in the first semester. However, this negative impact is greatly diminished by the end of the third semester partly because the students have adjusted satisfactorily to the challenges of college or because they have learned how to adequately manage their time. It was established that the kinds of activities the students are engaged in during the SNS use are the leading factor affecting academic performance. Of those activities, using SNS during a lecture or while studying is the foremost contributing factor to lower academic performance. This is due to "cognitive" or "information" bottleneck, a condition in which the students find it very difficult to multitask or to switch between resources leading to inefficiency in information retention and thus, educational performance.

An Analysis of Security Competitions for a Beginner's Guide

Gu, Burns, Rios, Jordan, Underwood

Security competitions are emerging as a new approach in security education and professional training. At universities, security competitions are gradually introduced into Computer Science curriculum to attract more students into the security area and prepare them for a career in the security field. The benefits of competition-based education were recognized in many studies. However, there are still many challenges for beginners to participate in the competitions. To help beginners to study and participate, this paper analyzed thousands of competition problems in over a hundred security competitions in the past three years. This paper identifies several important characteristics of the security competitions, including the main security areas and the fundamental knowledge and skills to solve problems in these areas. This paper presents the findings as guidance to beginners so that they can find their interested areas to study and practice.

Applying Nodal Governance to Combat Cybercrime: A Novel Approach

Wilson, Laidlaw

This paper will address the impact of the ever-increasing phenomenon of cybercrime in America. It will argue that cybercrime as a new genre of illegal behavior (criminality) is having a significantly negative impact on key aspects of America's national security, financial prosperity, and public safety. The premise of the paper is that the contemporary cyberthreat landscape is an evolving target surface with a growing cast of nation-states, transnational organized criminal organizations, and other criminal actors who are continually changing and updating their modus operandi to maintain an advantage over cybersecurity defenders. Moreover, as cybercrime incidents increase in frequency, harm, danger, and cost,

the cybersecurity programs of public and private sector defenders may be incapable of effectively countering the threat, and the resulting growth in scale of cybercrime will continue to challenge and possibly overwhelm the capabilities of the federal-centric national cybersecurity strategy currently employed to counter this threat. The increasing and invasive nature of cybercrime mandates a critical and urgent need for enhanced capabilities and increased levels of expertise in combating, preventing, investigating, and policing cybercrime incidents. This paper recommends that American policymakers continue to recognize the level of threat presented by this damaging and noxious form of crime and in response adopt policies that foster implementation of an overarching national cybersecurity strategy based on the nodal governance of security.

Curriculum Development for Teaching Critical Infrastructure Protection

David Oliver and Michael Haney

The critical infrastructure of the United States, from the electric grid to transportation, agriculture, and financial and government sector systems, has simultaneously grown more vast and more complex. So too has the challenge of protecting the infrastructure as an intertwined and interdependent system of systems. Recent years have seen a shift in perception and a growth of importance in critical infrastructure protection (CIP). The nature of the complexity of these systems and interdependency of sectors necessitates a multidisciplinary approach to educating the workforce needed to protect them. This paper outlines the objectives and efforts at one university to build a graduate-level curriculum that seeks to bridge the knowledge and communications gap between once stove piped educational disciplines: 1) information assurance and cybersecurity from the Department of Computer Science, 2) sector-specific engineering from the Departments of Electrical Engineering, Mechanical Engineering, Civil Engineering, and Environmental Science, and 3) infrastructure protection and homeland security from the Departments of Industrial Technology and Engineering Management. The efforts to date include the creation of a new cross-discipline course covering the fundamentals of critical infrastructure protection and the creation of a new graduate certificate. The certificate has been formed by requiring the new fundamentals course as well as a series of elective courses from various disciplines chosen for meeting several distinct and specific learning objectives. The certificate program further serves as a roadmap of elective courses to be used by students pursuing a Master's degree in various engineering disciplines. The specifics of these requirements as well as our motivations for choosing them are described in this paper.

Cyber Education outside the Cyber Space: the case of the Catholic University Institute of Buea

Ngatchu, Anye, Kwedeu, Butler

The purpose of this paper is to extend the growing body of research on cyber education, by reporting the experiences of a cyber security department cut-off from Internet access. The value of Cyber education is expressed even beyond the cyber space.

Design/methodology/approach

This qualitative exploratory study used semi-structured interviews and content analysis to collect a wide variety of rich data in order to demonstrate the need and possibility of cyber education, even without Internet access.

Findings

Willingness to learn and the hope of a fulfilled career were found to be the most significant factors for students' continual motivation. The presence of an eminent "force majeure" was seen more as an opportunity for novel explorations. In contrast to customary thinking, the

constructs of information security and assurance were fully fledged outside the cyber space.

Research implications/ limitations

These findings are evince of a practical and contextual application of the concepts of information security and assurance, which could be used by instructors to offer an insightful picture of these concepts. They suggest out-of-classroom approaches and and offline activities which could be integrated into cyber education courses to engage students at a different level. The study is limited by its context and methodological approach and as such generalizations would be per-mature. However, it offers a unique experience from with other researchers and educators could draw inspiration.

Cybersecurity Career Profiling

Morgan Andreanna Zantua

Professionalization of a cybersecurity workforce is under development from multiple perspectives. Government agencies, the military and academic institutions strive to standardize excellent curriculum and career pathways, certifications, job descriptions classifications are contributing to the effort. In its infancy is the development of statistically validated psychological profiles of candidates' possessing the talent, disposition and interest to excel in the rapidly maturing field and diversifying field of cybersecurity. To address this gap we propose to borrow from the well- established medical profession and utilize psychological profiling protocols tailoring a statistically validated career assessment tool to build cybersecurity psychological profiles of two markedly different cybersecurity career pathways. Once profiles are defined and validated we propose several Next Steps. Team members and industry partners comparing the psychological profiles can advise or refute a case to conduct additional profiling of additional cybersecurity career pathways. The assessment protocols and methodology will be disseminated to multiple communities at regional, national and international conferences to increase the diversity and numbers of talent entering the cybersecurity career pipeline.

Cybersecurity Education at Formal University Level: An Australian Perspective

William (Bill) Caelli, Vicky Liu

Cybersecurity studies at undergraduate/postgraduate level are offered at numerous universities in Australia. The level offered varies from a specifically named undergraduate/postgraduate coursework degree to usual IT or relevant degrees offering cybersecurity as a minor or major theme. A minority of universities do not offer any specific cybersecurity specific course while others offer such courses in association with industry organisations. Based upon an extensive analysis of published course/program data from university websites, chosen as the best data repository that would normally be examined by prospective students, this study submits that in Australia available courses are few and are acknowledged as not meeting market demands for skilled cybersecurity professionals. This has been recently recognised by Australia's Federal Government which has implemented the "Academic Centres of Cyber Security Excellence (ACCSE)" program in its 2016/2017 budget to proote the discipline and university support for it. In summary, courses currently available appear quite limited in scope.

Cybersecurity Training and the End-User: Pathways to Compliance

Dinesh Reddy, Srinivasan Rao, Glenn Dietrich

Erich Spengler Student Paper of the Year

In order to effectively combat cybersercurity threats at home and in organizations, it is imperative to achieve higher end-user cybersecurity compliance. Cybersecurity training is generally accepted as a means to increase

compliance behavior. Training can influence compliance by one or more of three causal pathways: by increasing cybersecurity awareness, by increasing cybersecurity proficiency (i.e., improve cybersecurity skills) and by raising cybersecurity self-efficacy. The effects of awareness and self-efficacy on compliance have been empirically examined and reported in literature, but the effect of cybersecurity skills has not received much attention. In an effort to understand the pathways through which training affects compliance, we develop a theoretical model and offer propositions. The model helps us understand how cybersecurity training should be designed and executed to optimally influence each of the three pathways to compliance and finally to have an optimal impact on compliance. Empirical validation will be performed at a later stage. Results of the study are expected to help design training programs to enhance end-user cybersecurity skills and consequently cybersecurity compliance.

Developing Postgraduate Cyber Security Programs at the Australian Centre for Cyber Security at the University of New South Wales Canberra at ADFA

Elena Sitnikova

In the modern world of exponentially increasing threats from advanced technologies, many institutions recognise the need for establishing cyber security programs to meet the growing demand for cyber security professionals in industry, government and defence organisations. However, cyber security, cyber defence and cyber war education is still ill represented in Australia. Some directions to overcome the problem is given by the Australian Government (Australia's Cyber Security Strategy)[1] but not yet fully developed. To address this issue, the Australian Centre for Cyber Security (ACCS) at the University of New South Wales (UNSW) Canberra at ADFA has been developing a suite of three postgraduate cyber security programs for the steadily increasing numbers of students from diverse backgrounds interested in studying cyber security and acquiring cyber warfare skills. The Centre is the only one in the world that offers a university degree specialising in cyber war and peace. This paper will describe the structured approach of developing the programs, highlight challenges by providing observations and lessons learned over the past two years, and propose some future directions on how to overcome these challenges.

Development in Training and Education for Australian Cyber Security: Filling the Gaps

Jill Slay, Greg Austin

There are several areas in the Australian cybersecurity ambition where key foundations or linking mechanisms are absent. There is a large gap between U.S. assessments of advanced technology threats and the Australian government's public assessments. These gaps have important policy implications, as well as negative impacts on the security and prosperity of Australians. The country's cybersecurity, cyber defence and cyber war education and training policy is foundational to the establishment, development and enhancement of every other cybersecurity policy in a civilian or defence context, and as guidance for the glaringly obvious national lack of a skilled workforce. Australia needs to make giant steps, of which an enhanced STEM approach is only one, and one that will have no strong pay-offs in the next decade at least.

Discovery of Insights on Cybersecurity Education Using Analytics from Twitter

Zenebe and Yorkman

There are enormous amount of data generated about various topic or organizations on several matters on cyberspace on a daily basis. We used IBM® Analytics™ for

theretrieval, extraction and analysis of social media contentson the topic Cybersecurity education. The contents were from Twitter, and the time frame selected was from January 1, 2015 to March 14, 2017. The trends of the tweets, distribution of the geographic locations and gender of the authors of the tweets were presented. Furthermore, in order to understand the tone of the tweets, results of sentiment analysis were presented including overall sentiments and sentiments by gender as well as by states for USA. Furthermore, the discovered insights such as sentiments can be used for recruitment/enrollments as well as retention of students in Cybersecurity education by institutions.

Educating Consumers on the Security and Privacy of Internet of Things (IoT) Devices: A Quantifiable Security Compliance Measurement System to Aid in Purchasing Decisions

M Khadeer, Dupuis, S Khadeer

As the adoption of technology grows, consumers have many avenues to buy IoT devices and install them for their needs yet they have very little information about the security of the devices. The companies that are manufacturing the devices have no incentive to invest in the security of the devices or to let consumers know the security status of their respective devices. The competitive cost and time pressure faced by manufacturers is causing consumers to suffer from the vulnerabilities in their devices. This project makes three contributions to the development of security verification for IoT devices. First, it develops a quantifiable security compliance measurement system to measure the security of consumer IoT (SCMSI) devices. The SCMSI framework uses the OTA recommended Trust Framework augmented with key design and development security concerns to develop the criteria to measure the devices. Second, a scoring model is developed for each of the security requirements in the SCMSI framework. Third, a consumer facing pilot website is built to show the proof of concept of evaluating IoT devices and providing security ratings to consumers. Limitations and future directions are discussed.

Identity Theft Education: FIT Report

Susan Helser

Identity theft losses are in the billions of dollars. The crime affects individuals and industry. It consumes valuable resources and results in higher costs across the board. Technical strategies to address the problem have had mixed effects. The focus of this work is to report outcomes from research that assessed two distinct educational methods that targeted identity theft at the college level. One mode of presentation is text-based while the other is game-based. Study data show that students exposed to information through the game-based approach scored better on the identity theft assessment than did their counterparts who experienced the same information through the text-based method. Also, game-based participants remained longer in the educational unit and reported greater satisfaction than their text-based counterparts. Digital educational game-based learning is in its infancy. FIT demonstrates the efficacy of this method in the field of cyber education.

Initial Steps Towards Assessing Cybersecurity Courses

Scott Bell

The past two decades have witnessed explosive growth of the Internet, cloud-based data storage, and widely connected mobile devices. This growth has led to a similar rise in cyber-related threats and thus a dramatic growth in university offerings of cybersecurity related content. One of the primary goals of this growth is to help attract and prepare a generation of cyber-defenders to take on this growing threat. However, there has been very little, if any, formal evaluation of how well these offerings are

achieving this goal. This paper presents the background of, and results from, the third phase in our development of a tool which can be used to assess changes in student interest in, and self-efficacy towards, pursuing jobs or additional education in cybersecurity. Phase one, which involved a qualitative study of students enrolled in a basic cybersecurity course, and phase two, which involved the initial development of the tool, have been explained in previous work and are described briefly in this paper. This phase involved collection of data over two semesters, providing us with a larger sample size and initial evidence of useful outcomes. The results from this first implementation are mixed, but the survey does show some interesting initial results. With additional work, it has the potential to allow educators to approach future improvement of pedagogy in cybersecurity courses in a more scientific manner. This work provides a starting point for discussions among those interested in building strong cybersecurity programs that produce successful graduates in this sub-field of Computer Science.

Searching and Developing Cybersecurity Talent

Barbara Endicott-Popovsky, Viatcheslav M. Popovsky

The lack of talent in the field of cybersecurity is keenly felt across all sectors of the economy - industry, government, military, academia [1]. While cybersecurity education has been a national priority, there still are thousands of cybersecurity jobs going unfilled and the gap will take a long time to close [1]. Of further concern, the authors have gathered anecdotal evidence that employers in both government and industry consider many recent cybersecurity graduates woefully unprepared for the realities of the workplace, taking too long to become effective. This paper describes one university's approach to address both the supply and preparedness problems, beginning with the application of the theory of pedagogical systems and methodology from sport and physical culture science and pedagogy to introducing the first iteration of a cooperative learning mode - inspired by this theoretical base and experience with its application - i designed specifically to develop and graduate 'breech-ready' cybersecurity professionals.

Smart TV Upgrade, Privacy Downgrade?

Michele Azar, Cindy Hoffman, Chueyee Fang, Abdifatah Abdi-Nur

The purpose of this paper is to create public awareness for privacy and to better protect consumers from Smart TV vulnerabilities. The analysis highlights many of the seemingly harmless Samsung preloaded applications that offer consumers little privacy. With the skyrocketing sales of Smart TVs, comes a critical challenge to protect customers' Personally Identifiable Information (PII). The need to educate and drive security awareness falls on both the private and public sector.Manufacturers, retailers, customers, and legislators need to help define the scope of protection required to mitigate the risk. This paper looks at the need to create public awareness for privacy and explore possible mitigation strategies to better serve and protect consumers from Smart TV vulnerabilities.

Teaching Cyber Resilience for Critical Infrastructure Systems

Conklin, Kohnke

Successful cyberattacks will occur no matter how much money and resources are dedicated to the problem. At the same time, the sectors in the current national infrastructure have not developed an effective standard strategy to protect themselves. The paradigm we present here argues that a *cyber-resilient* strategy is an effective and cost efficient approach to protecting the critical systems that power our way of life. This paper presents both a staged approach to implementing cyber-resilient systems as well as a general curriculum and pedagogy for disseminating this knowledge.

The Calculus of Cyber Warfare as Influenced by the Subtle Art of Military Theory

Shaw, Carr, Muehlelisen

Ever since The History of the Peloponnesian War as written by Thucydides, an Athenian historian who also happened to serve as an Athenian general during the war, we have intellectually feasted upon progressive war theories throughout the ages. Conventional war is generally considered a three-dimensional endeavor. With the advent of cyber warfare, we add a fourth dimension of silent, asymmetric proportions, normally conducted by nation-states waged against one another. This war is currently being fought on a global scale endangering the security of many States and organizations. We face a vicious cyber offense with no rules of engagement and defend with a cyber defense system that labors valiantly under layers of rules, regulations, and oversight that is legacy from decades back, slow to progress to match the speed and efficiency of the cyber threat.

The authors of this paper seek to address the cyber threat from a military perspective, adapting time proven strategic military theory and theorists concepts of conventional warfare to principles of cyber warfare.

Towards the Design of an Interdisciplinary Bridge Curriculum in Health Information Systems: A Pilot Study

Niya F Werts, Subrata Acharya

This research responds to the critical need to develop educational opportunities to facilitate interdisciplinary communication and field literacy to better prepare students in the health sciences and technology fields for more effective inter-professional collaboration as well as next generation workforce development. The product of this research has been evaluated by an external focus group and can be used by educators in developing a framework for curriculum development, implementation, and evaluation of an interdisciplinary "bridge" course, and avoid some of the pitfalls of interdisciplinary course development.

What Constitutes Core in a Cyber Security Curriculum?

William (Art) Conklin

Cyber security is an expansive domain that has components from many different disciplines. From the obvious computer science and information technology areas, to business, psychology, political science, law, law enforcement, and more, the list goes on. With the rise of programs such as the Centers of Academic Excellence in Cyber Defense Education, one of the key questions is "what constitutes an appropriate curriculum." A subset of this question is: what constitutes the core knowledge that is essential regardless of program specialty. This paper addresses this very question.

Presentations

A Novel Anti-Adversarial Compromise and Tamper-Resistant IoT/CPS Trusted Computing Protocol - IoTCP

Wang, Shumba, Kelly

The ability to understand, predict, secure and exploit the vast array of heterogeneous Network of Things (NoT) is phenomenal. With the ever-increasing threats to Cyber Physical Systems (CPS) and Internet of Things (IoT), security on those networks of datagathering sensors and systems has become a unique challenge to industries as well as to military in the battlefield. To address those problems, we propose a hybrid trusted computing protocol that employs firmware-based Trusted Platform

Module (fTPM) and Hardware Security Module (HSM) for establishing trust between devices and actuators. The IoT-based Trusted Computing Protocol (IoTCP) implements integrated hardware security and strong cryptographic hash functions. We investigate the protocol under various circumstances where devices have built-in securities while others do not. We evaluate and analyze the new protocol with a CPS system that contains more than 3,000 edge devices. the preliminary results show that IoTCP protocol establishes trust, improves security, integrity, and privacy.

A Survey on Online-Banking Security Models, Successes, and Failures

Abdu

An online-banking (OB) system allows bank clients to achieve all the account management and business transactions via the Internet [1]. The prevalence of the online-banking system is accompanied with an increase in the fraudulent OB transactions. Fraudulent OB transactions are now considered the reason of huge losses compromising all the system; this is due to the growth of severe OB threats such as Pharming, Man-in-the-Middle and Keylogger. Therefore, extensive search for advanced security models to secure such vulnerable systems needs serious attention. In this survey paper, we debate OB threats and their security mechanisms. In addition, recent and past related work are reviewed to point out failures of the existing OB security models – which lead to frequent attacks – and to achieve a fully developed security model to overcome this real dilemma.

An Early College Approach to Cybersecurity Workforce Development: Online Instructional Infrastructure, Student Support and the Improvement of Practice

Nakama, Haynes, Paullet, Yamanuha

This case study focuses on factors related to student access, teaching and learning, and student support for an online early college cybersecurity education career pathway. Additionally, it studied the specific problems that are part of the collaboration process and identified solutions to minimize their occurrence. High school students and major project stakeholders from schools, districts, businesses/industries and a hybrid community college were surveyed throughout the project cycle on their opinions on successes, problems, and solutions related to the university-high school collaboration model.

The intent of the case study is to figure out how and why things work (including their contextual constraints) not simply what works. This case study presents an exploratory research-practitioners and development design that specially focuses on improving opportunities for high school students to access and prepare for the cybersecurity workforce in rural communities. Overall, a major finding of this case study is that the Stakeholders were extremely positive about the value of the career pathway and its contribution. These Stakeholders would like to see the cybersecurity career pathway expanded to more high school schools.

Comparison of Randomness of SecureRandom and Trivium by using NIST's STS

Latoya Jackson, Yesem Kurt-Peker

A pseudorandom number generator (PRNG) is an algorithm that produces a sequence of numbers which emulates the characteristics of a random sequence. In comparison to its genuine counterpart, PRNGs are considered more suitable for computing devices in that they do not consume a lot of resources (in terms of memory) and their portability; they can also be used on a wide range of devices. Cryptographically Secure PRNGs (CSPRNG) are the only type of PRNGs suitable for cryptographic applications. They are specially designed to withstand security attacks. In this paper we provide

descriptions of two CSPRNGs: Trivium, a stream cipher designed for hardware efficiency, and SecureRandom, the CSPRNG recommended for Java programs that include a cryptographic algorithm. In this paper, we present results of NIST Statistical Testing Suite (STS) comparing statistical properties of the two generators. Our analyses indicate that even though SecureRandom performs slightly better under STS, the difference in performance is not significant. This hints that Trivium could be a viable option for pseudorandom number generation in space restricted environments.

Connecting the Boardroom to the Server Room: An Example of Using the KPB Model to Develop Capacity to Train Executives to Lead Cyber Preparedness and Response

Tom Muehleisen

The landscape of our modern cyber battlefield is littered with hulks of poorly prepared organizations who collapsed under the weight of some form of breach or attack. This short paper explores an example of the content being used to develop a course titled, "Continuous Cyber Resilience: Leading Transitions."

This course represents the capacity building portion of an NSA grant to provide cyber training to Army Reserve leaders. This example leverages their experiences as leaders and allows them to adapt their existing executive skills to the cyber context using proven military concepts of information management during crises and information protection during routine operations. While these concepts are complex in implementation, they are simple in concept and very adaptive to organizational context. This example uses two vignettes to show the stark difference between a surprised, immature organization and a prepared, mature organization.

The author seeks to demonstrate the expected viability of this approach to executive education using a proven model, KBP (see figure 2 below), and focusing on lessons learned by the University and its surrounding communities/state during the past 5 years.

Cyber Range Exploration - A Range of Possibilities

Guenther, Levesque, Ahvakana, DeRoest, DeLeon, Bold

Cyber Range Exploration – A Range of Possibilities grew out of our department's interest in the role cyber ranges and labs play in the rapidly expanding sphere of cybersecurity education. The increasing demand for cybersecurity programming translates to a greater use of online curricula and labs as well as both on prem and cloud-based ranges. We observed a variety of approaches by industry stakeholders and diverse expectations from campus stakeholders. Our inquiry began as an environmental scan of "what is" and ledto analysis of six sources of curriculum, ranges, and technology.

Cybersecurity as a Meta-Discipline

Ekstrom, Parrish, Sobiesk, Raj

The US Bureau of Labor Statistics projects employment in cybersecurity to grow much faster than the average for all occupations. This demand has resulted in a proliferation of training programs for a variety of cybersecurity-related specialties–offered in a variety of modalities, with a variety of training objectives, and from a variety of training providers. Although some programs are delivered via non-traditional training providers, others are delivered at various levels of a traditional university education. While the diversity of offerings has had some impact on the volume of the labor pipeline, higher education has generally been a marginal participant. A limitation within higher education has been a lack of consensus on the role,

scope, and position of cybersecurity within the landscape of academic disciplines. To address this problem, this paper proposes a path forward where cybersecurity is defined as a "meta-discipline." As a meta-discipline, cybersecurity reflects a family of disciplines, and as such, it differs in significant ways from computer science, information systems and information technology, or engineering disciplines such as computer engineering and software engineering. In fact, Cybersecurity may be more semantically similar to "Computing" than to any of the individual computing disciplines. This paper describes a clear framework for discussing cybersecurity, along with appropriate parameters and context for implementing cybersecurity in higher education, which is needed to ensure that an appropriate share of the cybersecurity workforce development burden is met by higher education.

Do You Have a Cyber Delinquent at your House? A Strategic Framework to Prevent and Intervene Teen Cybercrimes

Liu, Murphy, Conrad

Juniper Research predicted that rapid digitization of consumers' lives as well as organizational and government records will increase the cost of cybercrimes to $2.1 trillion globally by 2019, quadrupling the estimated cost of cybercrimes in 2015 (Juniper Research, 2015). Another report released by the Centre for Strategic and International Studies (CSIS) disclosed that, in the U.S. alone, cybercrime caused the loss of at least one half million jobs annually as companies struggle with the loss of intellectual property and suffer reputational harm (Center for Strategic and International Studies, 2013).

Cybercrime is becoming more prevalent due to several factors. Firstly, it is facilitated by affordable, easy-to-access 'crimeware' kits and programs. Cybercrime black markets have been burgeoning, where criminals can buy everything from free and accessible cyber attack toolkits to credit card numbers to email lists to online bank accounts[1]. Secondly, there are many motivations driving cybercriminals include making money, politics or ideology, sabotage, extortion, ego or vanity at being able to do it, taking revenge, and outrage trolling (IBM Security, 2016). Thirdly, cybercriminals, particularly those of a younger age, believe they are anonymous on the Internet, resulting in the disinhibition of online criminal activities and behaviors (Suler, 2004),both on an online and non-virtual platform (Kar, September 24, 2013).

Over the past few years, we have seen the people engaging in cybercrime becoming younger and younger. The Global Economic Crime survey conducted by PricewaterhouseCoopers (PWC) reported that cybercrime conducted by youth accounts for 38 percent of economic crime incidents compared to 16 percent for other industries (PRNewswire, 2014). It has been noted by international law enforcement communities that younger generations are increasingly committing cyber offenses and being drawn into cyber-criminality ranging from money laundering for criminal gangs to attacks using remote access Trojans (Harris, April 11, 2015; Kar, September 24, 2013; Peters, May 19, 2014). In addition to the aforementioned external factors driving youth cybercriminals, the behavioral science theories also shed light on this phenomenon. Well established in the field of behavioral sciences, impulsivity and risk-taking behavior is known to increase throughout the formative teen years (Aiken, Davidson, & Amann, 2016). Along with these issues, the availability of technology, information and virtual gaming or social communities have been hotbeds for deviant behavior and criminal activities.

Forensication Education: Towards a Digital Forensics Instructional Framework

Rick Kiper

The definitions of digital forensics seem to be as varied as the number of forensic examiners in practice. Recognizing this fact, the National Institute of Standards and

Technology (NIST) offered their own definition in *Guide to Integrating Forensic Techniques into Incident Response* [1]:

Digital forensics, also known as computer and network forensics, has many definitions. Generally, it is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data (p.15).

Similar to NIST, the National Initiative for Cybersecurity Careers and Studies (NICCS) provided a definition that focuses a bit more on the technical aspects of the job. According to NICCS [2], the digital forensics professional "[c]ollects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations" (p.1).

However, other notable sources seem to give at least equal emphasis to what happens *after the forensic exam is completed*

"Digital forensics is the process of acquiring, analyzing, and presenting relevant and admissible digital data from different data states in a forensically sound manner suitable for litigation support" [3].

With such a variety of opinions about the scope of digital forensics, it is not surprising that digital forensics instructors have failed to reach consensus on how to teach and assess mastery of its basic tenets. Some training programs provide hands-on learning experiences with a practical-based assessment, while others are mostly lecture-based, with assessments drawn from minutia buried in course textbooks. Some courses promote the presentation/admissibility aspect of digital forensics while others spend very little class time dedicated to legal considerations or reporting. There is simply no agreement regarding how to develop and implement the most important features of digital forensics instruction.

Integrate Insider Treat into Cyber Security Curriculum

Hongmei Chi

Insider threat is a major issue in cyber and corporate security. Insider threats pose a severe problem for any organization because it is difficult to prevent and damage is huge. The best way of protecting all aspects of an internal network is to monitor high-risk employees. However, in cyber security education curriculum, there are few papers to address this issue. Insider threats originate from people given access rights to systems and misuse privileges violating security policy. Interdisciplinary approaches to fight the insider threat are critical to train our students in college level. Integrating insider threat modules into cyber security education is the key to address this issue.

Meaningful Choices for Cybersecurity Education

Laurin Buchanan, Lori Scarlatos

We have developed a web application that enables subject matter experts to rapidly develop choose your own adventure comics for teaching cybersecurity topics to a wide range of students, from cybersecurity awareness for K-12 students and workforce education, as well as education for technical practitioners. Although engaging and informative for a wide range of students, web-based, educational choose your own adventure comics have been costly to produce, requiring programmers and graphic artists. The current work seeks to streamline the process for educators and remove the need for outside assistance. In particular, we (1) discuss our motivations and the pedagogical theories that support this approach; and (2) explore diverse ways this technology could be used for learning and evaluation both in and out of the classroom.

Mobile Security: A US Intelligence & Counterterrorism Dilemma

Robert Duhainy

The cyber terrorism is a real threat to fast technology development. Potential targets are systems which control the nation's defenses and critical infrastructure. The terrorist of the future will win the wars without firing a shot - just by destroying infrastructure that significantly relies on information technology. The current mobile security mechanism stands chance in exposing the existing vulnerabilities. The paper discusses the current technology behind mobile security and how it currently holds terrorism threat at bay. Valuable intelligence can and should be gathered from the message boards, chat rooms, and various sites but will pale in comparison to the intelligence that can be gathered from the terrorist's personal devices. A final direction for future research involves the development of efforts to counter the growing threat of cyberterrorism in an increasingly electronic-dependent world.

QuaSim: A Simulation-Based Instructional Tool for Learning Quantum Cryptography

McDermott, Vadla, Bommanapally, Parakh, Ostler, Subramaniam

Quantum cryptography is often looked upon as one of the more difficult and counter-intuitive subjects taught in a college curriculum. Furthermore, quantum equipment is expensive and while most computer science departments do not have access to it, traditional Physics departments teach a different kind of quantum theory. This project aims to bridge the gap using QuaSim. QuaSim is a gamified quantum cryptography educator that allows students to learn the counter intuitive concepts of quantum cryptography in a competitive setting. Built in Unreal Engine 4, it provides an immersive project based experience to students. The game mines student's gameplay data and builds a profile based on which it adapts to individual students abilities producing new puzzles in order to measurably improve learning. Students get awarded points for correct answers and lose "health" for incorrect attempts. Complete loss of health triggers an Oracle that intervenes to help and provide corrective suggestions. Students can also ask for hints from consultant at the cost of health.

Scare, Prepare and Dare: High impact, low cost incorporation of cybersecurity into high school curriculum

Uppuluri, Chase, Pittges

Given the pressing demand for a cybersecurity workforce, the goal of the *SPD* project at the [Anonymous] University is to increase the pipeline of high school students who plan to pursue Computer Science/IT as a major with cybersecurity as their focus. The two challenges we identified are (a) lack of qualified teachers - e.g., in the 20 school districts we surveyed in the state, there is no teacher with the skillset to offer a cybersecurity course, and (b) motivating students to consider CS/IT as a major – e.g., in the region that the University is located in, less than 250 out of 16000+ middle/high school students (across 4 school districts) take a CS/IT related course such as pre-AP or AP CS. This mirrors national trends. Even an introductory cybersecurity course that is rigorous requires students to have a wide array of foundational knowledge. Hence, cybersecurity programs in schools /colleges are multi-semester efforts where the first couple of semesters focus on the foundations – thus only drawing motivated students as it takes multiple semester before students actually work on security problems. In response to these challenges, with support from four NSA grants, the SPD is developing a curriculum that is exciting, rigorous and easy to adapt into high school classes. In SPD, by using an active learning strategy in the form of mini capture-the-flag (CTF) contests that drive the learning, students work on security challenges from Day 1 and the foundational

knowledge is introduced on a just-in-time basis. The curriculum is designed to be a bridge between the more basic cyber-awareness courses and the more rigorous multi-semester efforts. This paper describes the curriculum and its effectiveness. Specifically, the curriculum was taught as a graduate course for educators piloted in Spring 2016 for 24 teachers. Another 23 teachers took the course in Fall 2016. The educators who took the course overwhelmingly (94%) reported gaining the knowledge/confidence to teach security and 92% found the use of CTFs to be more useful in learning than a traditional lecture format.

The Potential Influence of Academic Degrees on Attempt Rates of CISSP Examination Takers

Pittman and Craft

The cybersecurity workforce is projected to have a shortfall in the tens of thousands over the coming years. While academia scrambles to produce skilled graduates, research has found that job seekers have turned to certifications to satisfy workplace conditions. One of the most common information security certifications for the workforce is the Certified Information Systems Security Professional. While existing literature has examined many aspects of the certification industry, there has been limited investigation into the role of academia has a preparatory mechanism for the Certified Information Systems Security Professional exam specifically. Thus, we questioned whether those with a graduate degree in information security or related field had a higher first-time pass rate for this examination. To answer, we collected data from 61 individuals and analyzed such using a correlational design. The results suggested that a significant, dependent relationship existed between participants holding a master's degree in information security or related field and passing the examination on the first attempt. Additionally, we descriptively analyzed the data as to provide a comprehensive overview of participants demographics. The findings may hold significance for educators, certification designers, and job recruiters. We also discuss recommendations based on the findings as well as ideas for future work.