Review Article

A Review of the California Cybersecurity Institute's Mission and 2018 Accomplishments

John Michael York[1,2,3*], Martin Minnich[3], James Baker[3], William J Britton[3]

[1]Rady School of Management, The University of California, San Diego, California, USA

[2]Institute for the Global Entrepreneur, Jacobs School of Engineering, The University of California, San Diego, San Diego, California, USA

[3]California Cybersecurity Institute, California Polytechnic State University, San Luis Obispo, California, USA

***Corresponding author:** John Michael York, Rady School of Management, University of California, San Diego, USA. Tel: +1-9494895570; Fax: +1-9492036115; Email: j1york@ucsd.edu

Abstract

Cybercrime has become a significant security issue for both the United States. California is a leading target for cyber-attacks, comprising 15% of the national total. Within the State, significant educational and workforce needs exist.

The State of California- through joint efforts between National Guard Cyber Protection Teams, California Military Department, and the California Polytechnic State University, San Luis Obispo (Cal Poly)- established the California Cybersecurity Institute (CCI) in 2016. The Institute defined its mission to support Cal Poly in becoming the leading supplier of cyber-ready professionals. The CCI's focus involves: (1) the education and empowerment of well-prepared, socially conscious, and career-ready students to be leaders; (2) the training of (service to) state, government, military, and law enforcement employees, along with its citizens; and (3) the develop research collaborations with faculty engaged in the cybersecurity.

In 2018, the CCI realized achievements in multiple areas, including: (1) the engagement of students through internships, University "Learn by doing" class projects, research efforts, and events; (2) the training of high school faculty via GenCyber; (3) the development of digital outreach technologies (e.g., an cybersecurity app on the Amazon Web Service platform); (4) the hosting of multiple education and training events; (5) the establishment of several corporate partnerships; (6) the securing of grants and credits from private and public sponsors to support education and outreach efforts; and (7) the establishment of a presence in the cybersecurity and general community through outreach activities.

The CCI has realized several accomplishments during 2018 and has gleaned many learnings from them, which will set the stage for future growth and achievements.

Introduction

Cybercrime has become a significant security issue for the United States and California. It is no longer a question of "IF" a cyberattack will happen on an organization, but "WHEN."

As the level of sophistication and devastation increase from cybercriminals, so must the training for the state of California and both current and future cybersecurity professionals. It is on the rise with no sign of stopping. The U.S. Government Accountability Office indicates that cybercrime has grown at a compounded annual rate of nearly 30% over the past decade [1,2]. This growth translates to 1100% in cyber-attacks [1]. In 2014 alone, the cost of cybercrime was $400 billion [3].

California is a leading target for cyber-attacks, comprising 15% of the national total [4,5]. In 2016, the State lost over $255 million due to cybercrime [4-6]. Over the last four years, cybercrime has steadily risen with a 25% compounded annual growth rate [5]. These statistics are very relevant to the mission and goals of National Guard, California Military Department (CMD), and Cyber Protection Team (CPT) to "improving, preparing, and protecting" the State of California. In California, the annual data account for cybercrime losses is estimated at $329 million, national security intellectual property loss, attacks on business, and attacks on critical infrastructure [7]. As the fifth largest economy in the world, the significance of the cyber threat to the State goes beyond its borders to both national and international implications [8].

The development of training programs for California's cyber defenders has not kept pace with the need to provide adequately skilled professionals. A recent study by Cyberseek stated that the US employs over 780,000 cybersecurity positions with an approximate shortage of an additional 350,000 current cybersecurity positions, with projections out to 3.5 million jobs by 2021 [9,10]. According to cyberseek.org, the State of California has 36,600 unfilled cybersecurity jobs [11,12].

To address these needs, joint efforts between National Guard Cyber Protection Teams, California Military Department, and the California Polytechnic State University, San Luis Obispo (Cal Poly, the Institute) established the California Cybersecurity Institute (CCI) in 2016 as a proof-of-concept. This effort was to demonstrate support for a stand-up organization to meet the State's cyber training, research, and workforce development requirements for the State of California to address its growing cybersecurity defense challenges [13,14]. The purpose of this paper is to examine CCI's initial mission, goals, and accomplishments. This article will discuss the CCI, review its mission and goals, and explore its 2018 achievements.

Methodology

During 2018, the CCI commenced several initiatives to develop and implement awareness, workforce development, and training concerning cybersecurity challenges and the prevention of serious sequala. The authors established this research to examine the initial progress with the Institute. Research for this paper involved reviewing documentation specific to the historical development, the Institute's mission and goals, along with its 2018 Annual report [13]. Findings from this exploratory research outline the Institute's current mission, along with 2018 accomplishments.

The California Cybersecurity Institute (CCI, Institute)

Overview

Established in 2016, the CCI is a robust, multi-agency response to address California's growing need for protection of its interests and residents from cybercriminals. Another charge that the CCI maintains is to prepare the current and next generation of cyber defenders through training and internship opportunities [13-15]. The Institute and Cal Poly aspire to become the leader in supplying well-trained cyber-expert professionals through a comprehensive and collaborative program that spans the University with public and private partners through the simple goal of education [13-15]. Finally, the CCI is to serve as a focal point for cybersecurity collaboration through strategic relationships with academia (e.g., Cal Poly College of Engineering Orfalea College of Business, and School of Journalism), government, and industry [13]. It strives to be a working proof-of-concept between academia, public, and private partners to meet the cyber training needs of the State of California [13-15].

Cal Poly intends to boast thousands of cybersecurity experts, at the undergraduate and graduate level, who can serve the cyber needs of society. The University is uniquely positioned to provide students with its "Learn by Doing" approach to education that will prepare them to make worthwhile contributions in the field of cybersecurity. Cal Poly sees the CCI as a part of its overall efforts through multiple entities to reach these goals. The University is staffing the CCI, building out its network, developing and acquiring courses, creating a state-of-the-art forensics lab, and forming critical private partnerships. The CCI will function as a platform and a venue for many types of activities that will allow Cal Poly faculty and students and law enforcement officials to develop and hone expertise. Through the full range of the CCI activities, Cal Poly's faculty and students will also be of service to the interests of the University community and society.

The Institute has established its headquarters adjacent to the campus Cal Poly at Camp San Luis Obispo [14]. The CMD and Cal Poly selected the San Luis Obispo central location so that it could be easily accessible within a day's drive to all of the state's 58 counties. The development budget for the CCI was between 3% and 5% of similar training centers nationally [14]. Its location is within the three buildings. The CCTC complex comprises over 120,000 square feet of space. This complex includes a forensics lab, operations, and training facility, and cyber range suitable for hosting large-scale, immersive training events [14].

Industry partners have donated thousands of dollars for cyber defense equipment for use by our staff, students, and faculty. Through a combination of training courses, grants, special events, donations, and research efforts, the CCI has been able to offer an attractive environment for students from both technical as well as liberal arts majors to "Learn by Doing." The CCI has worked with Cal Poly faculty to partner on cyber research and projects.

Mission and Goals

CCI fills a critical security gap by offering the capabilities to address local and State cyber capability needs (in italics) by providing [13]:

(1) A collaborative workspace (California Central Coast Forensics Lab, CCCFL) where cyber forensic professionals can share tools, learn new processes, and have access to resources that would otherwise be unavailable to individual law enforcement agencies-Forensic specialists often find themselves solving the same technical problem already addressed by other nearby agencies, and in many cases, they operate with outdated and underpowered equipment.

(2) A rigorous training and simulations center (which includes certifications through the Commission on Peace Officer Standards and Training for law enforcement and first responders), developed by experts in law enforcement and academic thought leaders in cybersecurity and related areas-Training is expensive and unavailable locally, forcing many agency staff to learn on their own.

(3) Resources and space for the practical development and testing of tactics to prosecute cybercrime in a realistic environment.There are areas for improvement for testing procedures and theories to predict how they will stand up to scrutiny in court.

(4) A setting for cyber defense innovation through advanced study, basic research, and applied research on emerging issues and technical challenges. Cybercrime is continuously evolving, but agencies responsible for fighting it need to have the latest knowledge and resources to stay ahead of the curve.

As education is the Institute's primary charge, the CCI currently offers a wide variety of live and online courses multiple times throughout 2018 and 2019. This curriculum will continue to evolve based upon the identified needs of the University's student and staff needs, the affiliated state agencies, the private sector, and the CMD.

The Institute's Vision, Mission, and Goals

The Institute defined its vision to create a world-class training and research facility dedicated to the complex and emerging cybersecurity challenges facing America, the State of California, and Cal Poly [13]. The CCI's mission supports the University in becoming the leading supplier of cyber-ready professionals. To achieve this effort, the CCI has established a comprehensive and collaborative program that spans the Cal Poly and partners with public and private organizations. The CCI's specific focus involves the of educating and empowering well-prepared, socially conscious, and career-ready students to be leaders.

Supporting this mission, the Institute seeks to educate and empower well-prepared, socially conscious, and career-ready students to be leaders by [13]:

(1) Producing cognizant graduates vis-à-vis academic, asynchronous, and live immersive training programs. All of these efforts ultimately create opportunities to ignite social change and create innovative, purposeful cybersecurity solutions no matter what their field or work.

(2) Enhancing the growth of the University through increased research projects, increased the desire for enrollment applications and expanded public and private partnerships via a Center for Security Studies. These efforts will have the ability to boldly address a security issue but also transform all the people involved.

To this end, the Institute embraces several core values:

(1) "Learn by Doing," vis-à-vis hands-on, student-centered, interdisciplinary education and an approach to continuous improvement in the field of cybersecurity.

(2) Excellence, as illustrated through a collegial community and industry partnerships that pursue responsive scholarship, innovation, leadership, and service.

(3) Knowledge, as evidence through scientific integrity, responsiveness to the security space, industry, and social needs through a dedication to fostering lifelong learning.

(4) Student Success, as demonstrated by students who are prepared to contribute to the diverse needs of society.

(5) Integrity as shown by the highest possible ethical standards and accountability for working in cybersecurity.

(6) Passionate professionalism, as reflected by respectful collaboration in collegial, industry, and government communities in the pursuit of excellence in teaching and learning, resulting in meaningful research and scholarship

2018 Accomplishments

In many ways, the Institute exists as a startup, or an entrepreneurial venture, within the construct of Cal Poly. Similar to many startups, CCI has had to establish a track record of accomplishment. In 2018, it realized achievements in multiple areas. The CCI has accomplished several critical stepping stones to success during the past year as well as set the stage for some exciting future accomplishments through the help of the faculty, staff, and students at the University.

Student Engagement

The CCI's goal is for student participation to be at the forefront of everything the Institute does. Students engage students through distinctive interdisciplinary learning opportunities through class projects, senior projects, employment opportunities, and professional internships (Table 1) [13]. Student contributions support of daily operations, event planning, digital evidence creation, narrative content creation, live action and roleplay in an immersive environment for training, app development, data analytics, cyber training events, cybersecurity research, and outreach.

Architectural	Created building and room drawings for the CCI;s facilities as well as mock-ups for training scenes.	++
Business	Participated in project management, business development, and event planning.	+
California (CA) Department of Justice (DOJ) Warrant Data Analysis	Used tools to clean and analyze data for the CA DOJ eCrime office. Agency to use results in a Supreme Court Case.	+++
	Used tools to clean and analyze data for the CA DOJ eCrime office. Agency to use results in a Supreme Court Case.	+++
CCIC - Digital Forensics Challenge	Redesigned CA Department of Justice forensic manual, designed the digital forensics challenge and created evidence in virtual machines. Worked on set design, script development, evidence creation, live acting, and roleplaying.	+++
Construction	Participated in set design, permits, plan submission and review with the base fire marshal.	+
Digital Production	Created multiple promotional videos for California Cyber Innovation Challenge (CCIC) as well as developed and maintained the CCI's website pages.	+
Forensics in the Cloud	Created a digital forensics computer assistant app in the cloud and developed forensics dashboard.	+++
Graphic Art and Design	Created straightforward and consistent marketing materials, along with infographics in compliance with Cal Poly branding guidelines.	+
Interior Design	Fully integrated the classroom spaces into a functional and inviting learning environment. Also incorporated the San Luis Obispo Museum of Art into providing artwork on a rotating basis.	+
Journalism	Developed backstory and current stories for our blog and outbound content.	++
Marketing	Designed a multifaceted marketing plan, competitor analysis, and social media marketing strategy.	++
PR Strategy	Developed a public relations plan to ensure consistency of messaging and selective targeting.	++
Research	Provided research assistance for cybersecurity grants.	++
+: Supportive of CCIs efforts; ++: Cybersecurity-related; +++: Significant cybersecurity activity.		

Table 1: California Cybersecurity Education Institute (CCI) 2018 Projects Involving Cal Poly Students [13].

First, the CCI employs between 12 and 15 students part-time during the academic year and gain invaluable exposure and training in a real-world setting. From January 2018 through June of 2018, the CCI employed four College of Engineering students, four College of Liberal Arts students, and two College of Education students. These individuals participated in several essential initiatives: (1) the Digital Forensics Challenge; (2) the Forensics in the Cloud program; (3) the California Department of Justice warrant data analysis project (research that the agency for use in a Supreme Court Case); (4) the production of digital communications (e.g., social media and web); (5) the development of the CCI facility and training scene mock-up architecture; and (6) the conduct of research.

Second, the Institute engaged 65 additional students and faculty across multiple colleges (business, engineering, and journalism) through Cal Poly's "Learn by Doing" pedagogy and instructional programs. These efforts incorporated faculty and class-led projects into efforts to address multiple areas of need. The CCI engaged students in various cyber training workshops and events. Additionally, the Institute provided students an avenue to earn "cyber certifications" through the more than 30 certifications that it offers onsite and online.

Third, the Institute has fostered student scholarship and significant student success. Notable examples involve that of Brian Kinnee and Sylvia Romero, recent Cal Poly graduates. Kinne had majored in English and worked with the CCI and Digital Transformation Hub powered by AWS last year. He helped to write the portion of the digital case library on Blockchain and presented a paper on this topic at a technical conference in Boston, MA. He received numerous accolades on his presentation and is now pursuing a Ph.D. in cybersecurity at the University of Washington as a result of his exposure to the CCI and cybersecurity. Romero was a recent grad from Orfalea College of Business, who majored in finance. She interned at the CCI in a business development capacity. The combination of her internship, brief experience in cybersecurity, and finance degree led to a job offer at Oracle this past year.

Online Library

As the cybersecurity field continues to change and expand, the CCI's goal is to provide students and faculty with a class resource that will foster a deeper understanding of issues in cybersecurity and their real-world consequences. As education is the Institute's primary charge, it created a robust library of educational offerings including courses and cases.

Concerning courses (Table 2) These, in particular, include over 40 online courses that students and community professionals have engaged with these offerings. This curriculum will continue to evolve based upon the identified needs of the affiliated state agencies and the CMD.

• GenCyber Training for Middle and High School Teachers • Cyber Protection for Vehicular Vulnerabilities • Cyber Strategies to Combat Human Trafficking • Cyber Strategies for Decision Makers • Digital Forensics for First Responders • Mobile Digital Forensics Examiner Training • The ecosystem of Mobile Forensics • Certified Information Systems Security Manager – CISSM • Certified Information Systems Security Officer – CISSO Certification • Certified Information Systems Risk Manager – CISRM • Certified Incident Handling Engineering - CIHE • Incident Handling for Laptops • CISSO Certified Information Systems Security Officer • CPTE Certified Penetration Testing Engineer • CPTC Certified Penetration Testing Consultant • CDRE Certified Disaster Recovery Engineer • CDFE Certified Digital Forensics Examiner • CNFE Certified Network Forensics Examiner • CSWAE Certified Secure Web Applications Engineer • CIHE Certified Incident Handling Engineer • CWSE Certified Wireless Security Engineer • CSAP Certified Security Awareness Principles • CVA Certified Vulnerability Assessor	• CISSM Certified Information Systems Security Manager • CISSA Certified Information Systems Security Auditor • CHISSP Certified Healthcare IS Security Practitioner • CISRM Certified Information Systems Risk Manager • CSP Certified Security Principles • CSAP Certified Security Awareness Principles • CVE Certified Virtualization Engineer • CVSE Certified Virtualization Security Engineer • CCSC Certified Cloud Security Consultant • CVDE Certified Virtual Desktop Engineer • CISS Certified IPv6 Security Specialist • CVFE Certified Virtualization Forensics Examiner • CPCE Certified PowerCLI Engineer • CVP Certified Virtualization Principles • CCSO Certified Cloud Security Officer • CISMS-LA Certified Info Security Management • Systems Lead Auditor • CISMS-LI Certified Info Security Management • Systems Lead Implementer • ISCAP Info Systems Certification and Accreditation Professional • CSAP Certified Security Awareness Principles • CSLO Certified Security Leadership Officer • CPEH Certified Professional Ethical Hacker

Table 2: The Institute's Education Offerings for 2018 [16]

Complementing the course offering, the "Cybersecurity Case Library" (CCL) provides another significant online offering created in 2018. This effort involved the creation and publishing of an undergraduate research journal (https://tinyurl.com/digital-case-library) that explores contemporary topics in cybersecurity. The CCI assembled students from multiple disciplines to co-write case studies regarding specific cyber events with the purpose of educating students campus-wide about cybersecurity. The case library featured articles including the following topics: (1) posthumous harm and privacy; (2) blockchain; (3) cyber threats in autonomous vehicles; (4) ethics and doxing; and (5) prosecuting cyber-attacks on cloud computing. The CCI planned the CCL 2019 editorial calendar to include case topics of interest including vehicular vulnerabilities, medical security enclaves, and digital ethics. The success of the CCL has involved its use by other universities around the country.

Training Programs

Building on its mission to train students, the Institute has focused on developing and implementing training programs in the community. The CCI, as an Institute of the College of Engineering, provides opportunities for training, research, and studies in cybersecurity.

Over the last year, the CCI with students and Cal Poly faculty developed cyber training for K-12 teachers, digital forensics, medical, anti-human trafficking, digital privacy, and vehicular vulnerabilities. One of the most notable was the GenCyber Initiative, a June 2018 program held that involved the training of high school teachers on cybersecurity.

Digital Technology Development

The Institute supports innovation as part of Cal Poly's efforts to foster entrepreneurship activities. The most notable was the development of digital outreach technologies. In working with Amazon through its Amazon Web Services (AWS) function, the CCI, in coordination with students and faculty, created a cybersecurity app (Figure 1).
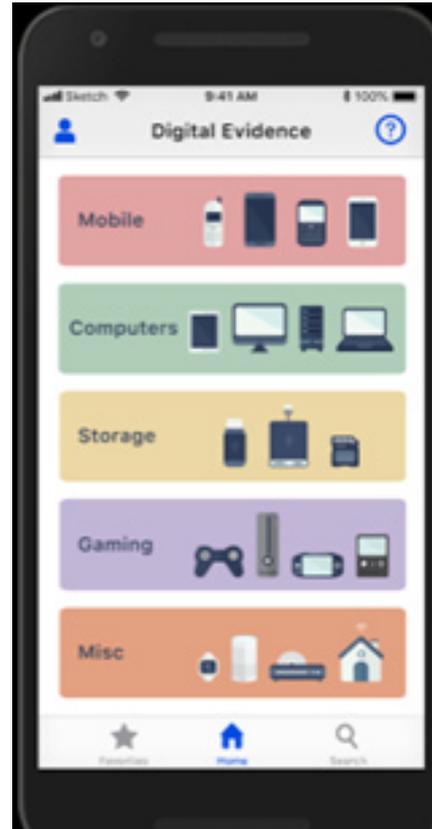
Figure 1: CCI Cyber Web App

Event Hosting

The CCI created several cyber-related events for the community, state, and Cal Poly students over the last year. Notable functions hosted at the CCI in 2018 included: (1) Law Enforcement Technology Advancement Day (May 2018); (2) *Women in Cyber* (May 2018) (Figure 2); (3) Cyber Workforce Summit (June 2018); (4) California Cyber Innovation Challenge (CCIC, June 2018); (5) GenCyber Training for Educators (June 2018); and (6) Multiple visits from congressional leaders and critical State of California delegates and legislators.
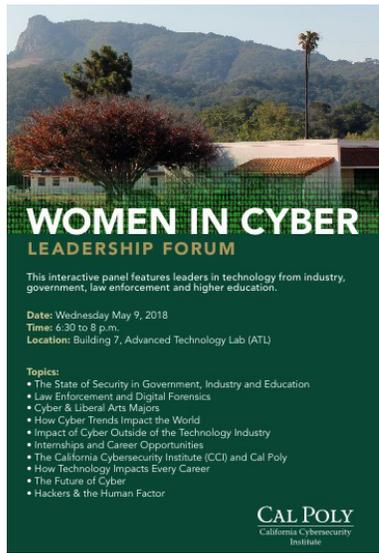
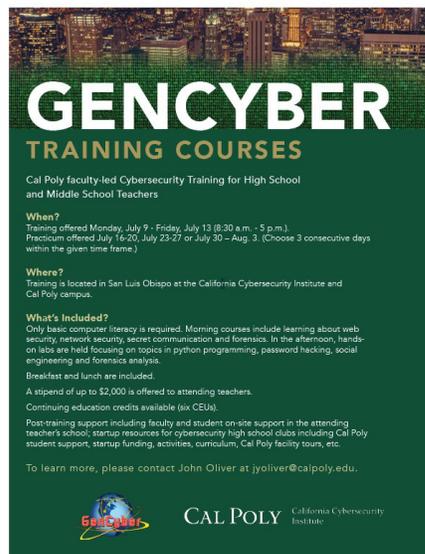**Figure 2:** Promotional Flyer for One of the CCI's 2018 Events, The Women in Cyber Leadership Forum.

Figure 3: Promotional Flyer for the CCI's Online Gencyber Training Course.

Feedback from one particular program, *Women in Cyber,* was incredibly supportive:

(1) "After attending this conference, my interest in cybersecurity and the entire cyber field grew. I found that there are so many different opportunities and career paths available…"

(2) "Before listening in on this leadership panel, I did not expect to learn as much as I did. Walking in, I saw 12 women that are involved in cybersecurity in their everyday jobs…"

The CCIC was another program that stood out as a tremendous success. Funded by the State of California's Go-Biz office, along with technology and medical organizations, the 2018 event was the second time that the CCI had hosted these events. The program featured 19 high school teams and one junior high school team for a total of 116 students. The teams competed in an immersive, cyber challenge around medical security that highlighted the issues involved with ransomware impacting many medical organizations throughout the country and digital forensic challenges throughout the day. Students were exposed to an immersive training environment and had to present their findings to a panel of academics, public service, and private function figures in this competitive event.

Partnerships and Grants

During 2018, the CCI efforts focused on building several corporate partnerships and grants, seeing grant wins with several private organizations;

(1) Amazon: The most notable collaboration involved the setting up of an Amazon Web Service (AWS) presence on campus via the Digital Transformation Hub (DxHub), an innovation engine where students work on real-world challenges in the public sector. The CCI's and Cal Poly's relationships with AWS was set up as one of a select engagement with an academic institution in the United States. Amazon AWS donated credits for the Institute to use for research, development, and training. Three students embarked on multiple training tracks via Amazon to educate and worked directly with law enforcement and first responders.

(2) Bugcrowd: This cybertech firm partnered with the CCI through the funding of internships and creating "Learn by Doing" events with the Cal Poly student body. The CCI's initial Bugcrowd sponsored student was learning penetration testing and ethical hacking, including the Bugbash Hackathon on the Internet of Things.

(3) Cisco: This national tech leader has been an active partner over the last year and donated a suite of lab equipment and full account access to Cisco Net Academy to help us continue to expand our curriculum library. This lab will be utilized to teach the Grizzly Youth Academy (a state-based program to help provide opportunities to disadvantaged and truant youths in the community) the basic of cyber fundamentals and digital literacy. Cisco Research Center University grant awarded for research on "Critical Infrastructure and Cyber."

(4) CrowdStrike: As one of the industry's leading cyber threat intelligence firms, CrowdStrike began to actively provide the CCI with regular updates on current threats and actors. Additionally, the company offers marketing support for the Institute's engagements throughout the year.

(5) MSAB: This industry pioneer provided an entire suite of mobile digital forensics software and hardware that allows for the extraction and examination of cell phone data. This equipment has been utilized for our live immersive set designs and in classroom instruction. MSAB has also generously donated financial and marketing support for a multitude of events.

(6) Oblong Industries: This innovative technical communications firm provided a system that allows for remote distance learning. The CCI has integrated the system the student learning and community training environment, along with student-developed an award-winner (2019 AVA Digital Award) video discussing how the system facilitated collaborative learning.

Adding to these partnerships were grant funding and support credits (e.g., Amazon, Cisco Research University, and Go-Biz) to support education and outreach efforts.

(1) California State Government Support: For the second year in a row, the CCI obtained grant support State of California Governor's Office of Business Development, via GoBiz.com, for the CCIC.

(2) National Security Agency: This entity awarded a cyber-grant to train high school teachers on cybersecurity. The classroom training for GenCyber utilized the new classrooms at the Partnerships and Grants.

Community Presence and Outreach

The Institute has engaged with the State and the local cybersecurity community. Various event sponsors and California government agencies have had the staff to speak on behalf of the Institute and the topic of cybersecurity. The CCI presented as at the 2018 University of California, Office of the President (UCOP) Oakland Cybersecurity Summit. Furthermore, State agencies have asked the CCI to participate in 2019 UCOP's Cybersecurity Summit in San Francisco and Santa Barbara as well as in the planning stages of a cyber-summit at the CCI for UCOP leadership. Furthermore, the State of California's Annual Cybersecurity Education Summit featured Minnich as a keynote speaker on the closing cyber panel.

For future presentations, multiple organizations have extended to the CCI invitations so it can present as part of various law enforcement and justice events (e.g., SoCal Justice and Public Safety Working Group and Orange County Sheriff's Quarterly Working Group). California Peace Officers Association has requested the CCI to conduct sessions at the Cops West conference in August of 2019.

Additionally, the CCI has been active in several other local and State programs. The Institute has engaged with government and law enforcement events hosted by InfraGard on cybersecurity. The Governor's Cybersecurity Task Force and Subcommittees have asked the CCI to be an active participant. Finally, the Institute has been active in participating in several industry conferences (e.g., RSA Risk & Cybersecurity Services, BlackHat, NICE, and DEFCON) and projects (e.g., DEFCON Biohacking Village). The CCI has been working with the California District Attorneys Association (CDAA) on hosting training on the dark web. Finally, the CCI has been part of numerous groups focused on fighting human trafficking including the Central Coast Freedom Network, Freedom Calling, and the San Luis Obispo County District Attorney's Office Human Trafficking Task Force.

Other Notable Accomplishments

Finally, the CCI has achieved several other achievements in 2018. The most notable was when the College of Engineering's Dean Amy Fleischer, along with the CCI's Director William Britton, hosted the Hewlett Foundation at the CCI.

From a staffing perspective, the CCI transitioned former Program Manager Bruce Burton into a consulting role and brought in new Program Manager Martin Minnich during 2018.

Finally, Danielle Borrelli, a manager at CCI, was recently awarded the Cal Poly Employee of the Year Award (and Assembly District 35's Woman of the Year) for her work at the CCI, as well as community efforts both in San Luis Obispo and internationally, to combat human trafficking.

Conclusion

The CCI is focused on a severe and growing problem for the State of California by addressing the cybersecurity defense and workforce shortage. As with any startup, the CCI has accomplished several critical stepping stones to success during 2018 that support its vision and mission through the help of Cal Poly faculty and students and the CCI staff. The CCI continues to emphasize student participation at the forefront of everything it does while addressing the training and research challenges facing government, law enforcement, military, and education communities within the State of California. The efforts of faculty, staff, and students of Cal Poly, and supports from private and public entity partnerships have aided the accomplishment of these efforts. The CCI has been on the path to sustainable growth through a combination of funding avenues via the State of California, grants, donations, and volunteer efforts. The Institute has gleaned many learnings from its 2018 accomplishments, which will set the stage for some exciting achievements in the future.

References

1. Wilshusen GC (2015) Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems. The United States Government Accountability Office.

2. Smith S (2017) 2017 Internet Crime Report. The United States Federal Bureau of Investigation. Internet Crime Complaint Center (ic3).

3. Thompson C (2014) Cybercrime Costs Global Economy $400 Billion: Report.

4. Coleman RC (2015) 2015 Internet Crime Report. The United States Federal Bureau of Investigation. Internet Crime Complaint Center (ic3).

5. Harris K (2016) California Data Breach Report. California Department of Justice.

6. Smith S (2016) 2016 Internet Crime Report. The United States Federal Bureau of Investigation. Internet Crime Complaint Center (ic3).

7. Watts T (2018) Cybercrime in America-Which State Is Most at Risk in 2018? Website Builder Expert.

8.   Associated Press (2018) California is now the world's fifth-largest economy, surpassing the United Kingdom.

9. Morgan S (2017) Cybersecurity Jobs Report 2018-2021. CSO from IDG.

10. Morgan S (2017) Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021: The cybercrime epidemic is expected to triple the number of open positions over the next five years. CSO from IDG.

11. Carrese J, Gross M, Hermann A, Ngo Bartel T, Greaney KC, et al. (2018) Cybersecurity Labor Market Analysis and Statewide Survey Results from California Employers and Postsecondary Institutions. The California Community Colleges. California Advanced Supply Chain & Diversification Effort. California Governor's Office of Business and Economic Development.

12. CyberSeek. Cybersecurity Supply/Demand Heat Map.

13. Britton B, Minnich M (2018) 2018 Annual Report: Cal Poly California Cybersecurity Institute. California Cybersecurity Institute California Polytechnic State University.

14. The California Military Department/Cal Poly (2016) California Cyber Training Complex Plan.

15. Bilk R, Larsen D (2013) Resolution on Proposal for the Establishment of the Cal Polycyber Security Center. AS-760-13. Academic Senate of the California Polytechnic State University, San Luis Obispo, CA.

16. California Cybersecurity Institute Course Catalog.