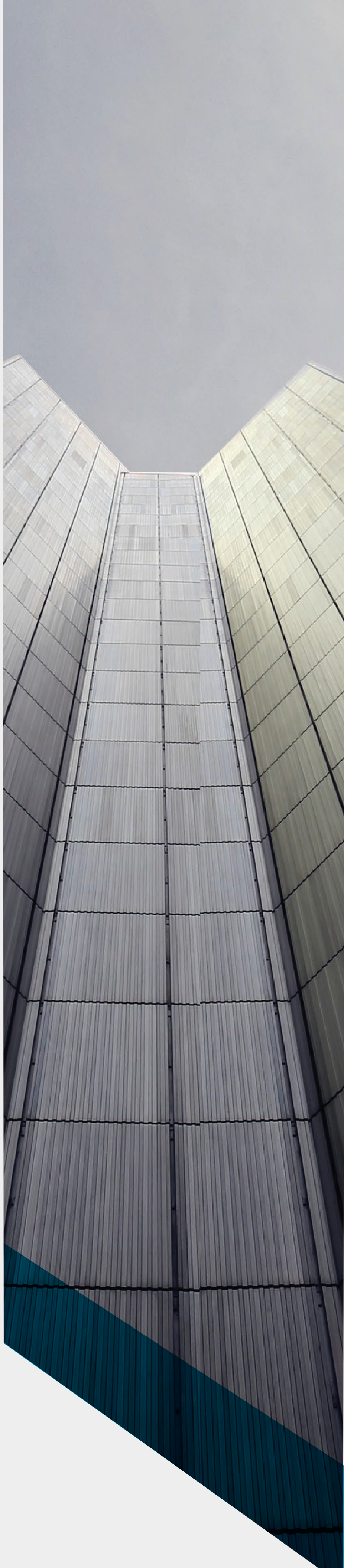
2016 - 2017 ANNUAL REPORT

NATIONAL CYBERWATCH CENTER

NATIONAL
CYBERWATCH
CENTER

www.nationalcyberwatch.org

CONTENTS



About National CyberWatch Center

National CyberWatch Center is a National Science Foundation-funded cybersecurity consortium working to advance cybersecurity education and strengthen the national workforce. Since 2005, National CyberWatch has played a key role in developing, promoting, and providing cybersecurity education solutions for the nation.

To learn more, visit **www.nationalcyberwatch.org.**

Hard copies can be ordered by contacting us at: info@nationalcyberwatch.org

EXECUTIVE DIRECTOR'S **MESSAGE**

Dear Colleagues,

In October 2016, the National Science Foundation awarded Prince George's Community College a $4.8 million National Advanced Technological Education Center continuation grant for its National CyberWatch Center project. The grant, which runs from October 1, 2016 - September 30, 2021, allows National CyberWatch to build on a 10+-year foundation of success, as evidenced by four successive National Science Foundation grants since 2005.

National CyberWatch continues to be the go-to organization for innovative, scalable, and cost-effective cybersecurity education partnerships and solutions. Some notable successes include:

- Creating, promoting, and validating performance-based credentials. The National Cyber League Scouting Reports measure strengths and weaknesses of both individuals and teams amongst various industry-recognized cybersecurity learning objectives

- Developing the first Information Security curricula to align instructional design, skill practice facilities, cybersecurity professional job performance standards, national workforce frameworks, and industry needs, which are desperately needed to guide responsible curriculum development for the new generation of Information Security specialists

- Establishing the National CyberWatch Curriculum Standards Panel. The mission is to identify the learning objectives, concepts, procedures, situational judgments, and intellective abilities required to successfully complete five courses currently available as digital courseware from National CyberWatch

These successes, combined with the other National CyberWatch programmatic results and impact, would not have been possible without our academic member schools (over 200+ nationally), faculty, students, industry and government partners, the senior leadership team at Prince George's Community College, and the dedicated National CyberWatch team members. We are also grateful to our Industry Support members, our National Science Foundation Program Officers, Dr. Corby Hovis and Dr. Victor Piotrowski, and our National Visiting Committee members.

As the daily barrage of compromised personal information and organizational attacks continues to dominate news cycles and social media, a growing portion of this attention is focused on the ongoing demand for qualified cybersecurity talent. Unfortunately, most organizations are looking in the wrong places for the talent they need, often with misaligned job requirements and credentials, outdated modes of recruiting and hiring practices, and a general lack of understanding of both the cybersecurity landscape and the threat models that affect them.

If we as a community are to tackle the cybersecurity human capital problem, it will require a different approach to recruiting and hiring, more nuanced discussions of required credentials, and programs that can serve traditional students, existing IT professionals, and workers seeking new and more prosperous career opportunities. More efficient talent management systems need to be developed by providing pathways for graduates of workforce training programs directly into middle-skill jobs representing the vast majority of the forecasted cybersecurity capability need by 2020.

Organizations that can develop and acquire the talent they need are at a distinct competitive advantage in today's marketplace. National CyberWatch has been at the forefront of developing and validating novel solutions to our cybersecurity workforce challenges since 2005. Moving forward, you can expect the same high-quality work as we lead collaborative efforts to advance Information Security education and strengthen the national cybersecurity workforce.

Best regards,

Casey W. O'Brien
Executive Director & Principal Investigator

MAJOR **EFFORTS**

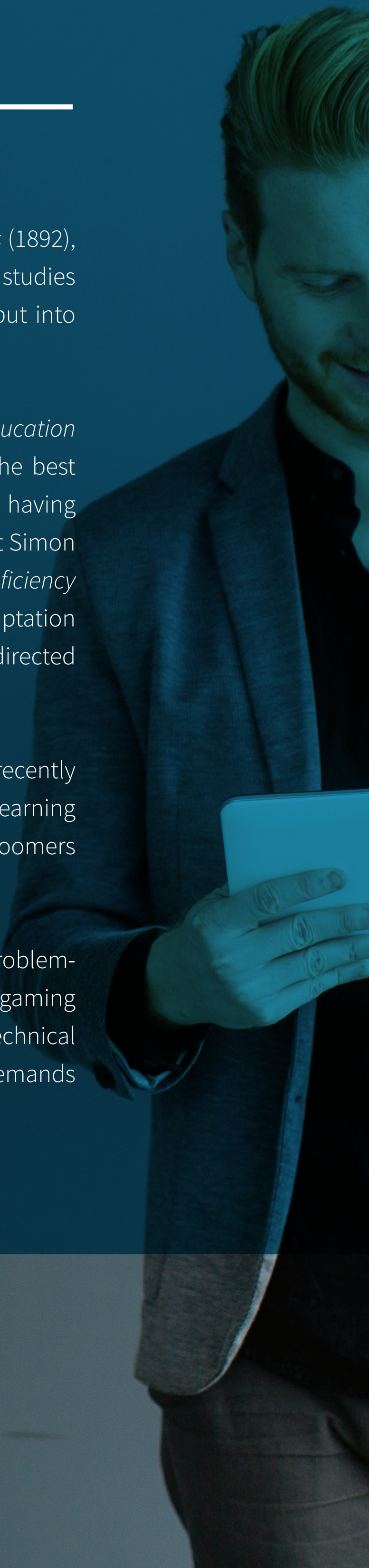
Practice-Based Education

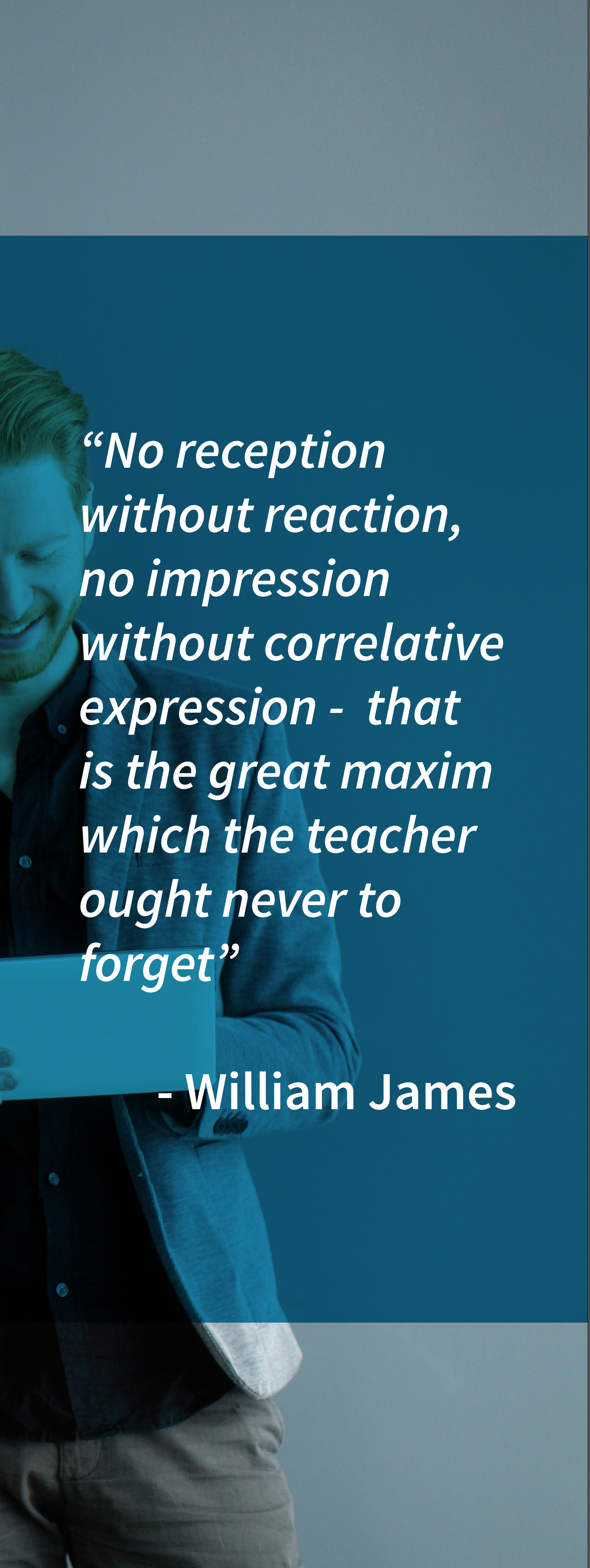
The statement on the next page from famous psychologist, William James, in his *Talks to Teachers* (1892), established the need for evidence-based, practice-centered education. James cited psychological studies showing teachers must ensure instruction is enacted, and newly received knowledge must be put into practice, or expressed in behavior, for education to be effective.

Nearly a century ago the founding father of modern education, John Dewey in *Democracy and Education* (1916), referred to this practice-centered pedagogy as learning by doing. Dewey argued that the best method for developing critical thinking skills is the use of problem-solving exercises. Yet, despite having laid the groundwork, it took a preponderance of evidence accumulated by Nobel laureate Herbert Simon and his associates, and a seminal workshop publication, Hoffman & Feltovich's *Accelerated Proficiency and Facilitated Retention (*2010), to clearly demonstrate that deliberate practice - the effortful adaptation of behavior in response to feedback when applying knowledge in a reasonably challenging goal-directed performance activity - is the most effective means to develop expertise.

From this evidence-based foundation, a **practice-based pedagogy for education (PBE)** has recently emerged. The initial problem that PBE seeks to solve is the unprecedented need to accelerate learning curves to address the growing skills gap created by the rapid loss of experienced workers as baby boomers retire in record numbers. This challenge is most acute in Cybersecurity.

The PBE solution to the cybersecurity workforce skills crisis combines work practice analysis, problem-based classroom or virtual instruction, and adaptive personalized simulation, using serious gaming technologies. The result is a work-integrated learning environment that links career and technical education with workplace learning programs to develop the labor pool required to meet societal demands for a competent workforce.





> *“No reception without reaction, no impression without correlative expression - that is the great maxim which the teacher ought never to forget”*
>
> **- William James**

Accelerated **Learning Programs**

The National CyberWatch accelerated learning programs integrate validated assessment, instruction, practice labs, and challenge scenarios to improve cybersecurity talent management in organizations.
Many opportunities exist for the National CyberWatch education and credentialing solutions to be enhanced by tight alignment with industry partners. Examples of collaborative opportunities with industry include:

1. Assess the capability maturity and related risk of the current IT workforce to identify risk and produce Individual Development Plans (IDPs)

2. Raise capability maturity of organizations by applying the IDPs to produce personalized instruction, simulated practice, and formative credentialing solutions

3. Select and develop a more capable entrant workforce through a residency program (similar to medical professionals) involving IDP-prescribed job rotations and validated, performance-based assessments

1ST CURRICULUM STANDARDS FOR **CYBERSECURITY EDUCATION**

Established in 2016, the National CyberWatch Curriculum Standards Panel-produced standards will be the first to align instructional design, skill practice facilities, cybersecurity professional job performance standards, national workforce frameworks, and industry needs, which are desperately needed to guide responsible curriculum development for the new generation of Information Security specialists.

The first project of the Curriculum Standards Panel was the **Cybersecurity Core Curriculum Mapping Project**. This project involved eight online working sessions with synchronous and asynchronous activities. Over 100 faculty, industry professionals, and government representatives volunteered to serve in support of establishing the nation's first curriculum standards for cybersecurity education.

The Cybersecurity Core Curriculum Mapping Project will be the first of several planned initiatives to produce formative credentialing solutions that increase the number of capable cybersecurity professionals protecting our nation from cyber incursion and increasing the reliability and effectiveness of the computing infrastructure critical to our national security and economic prosperity.

AWARDS & RECOGNITION **PROGRAM**

The National CyberWatch **Innovations in Cybersecurity Education** program is built on the premise that National CyberWatch members produce some of the best cybersecurity educational and workforce development innovations, and that through National CyberWatch, they can share their innovations, accelerate their adoption throughout the academic community, and receive proper recognition for their work.

Recipients of the first Innovations in Cybersecurity Education awards will be recognized at the 2017 Community College Cyber Summit (3CS), June 28-30, 2017 at National Harbor, MD.

NATIONAL INFRASTRUCTURE FOR A **REMOTE VIRTUALIZATION LAB ENVIRONMENT & CONTENT**

National CyberWatch has partnered with Baltimore-based Infosec Learning to develop a hands-on, scalable, and customizable virtual lab platform - **lab.nationalcyberwatch.org** - that supports skill development in any degree, certificate, training, or assessment program. The virtual lab platform provides an unmatched turnkey solution with real world tools and technologies.

This lab solution solves faculty and student needs in the following ways:

- No up-front cost to the school, nor any on-going fees
- Cloud-based infrastructure, allowing schools to begin using it immediately
- Hundreds of virtual labs mapped to many National CyberWatch courses, professional certifications, and various frameworks
- Step-by-step lab tutorials with corresponding virtual machines
- All HTML 5, no plugins needed
- Instructor analytics allowing faculty to see the activity of their students
- Learning Tools Integration (LTI) into the school's Learning Management System (LMS), allowing for single-sign-on capability
- Ability to update and distribute content seamlessly, without effort from the school
- Tech support: 7 days a week (8am – Midnight)
- Capture the Flag-type Challenge Labs with auto-scoring

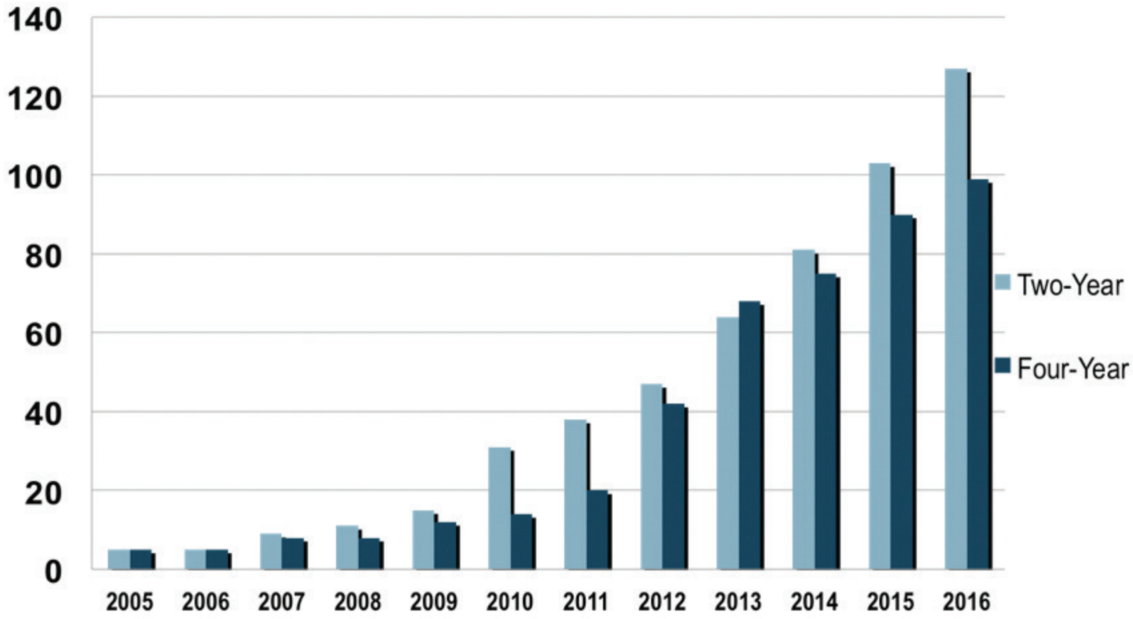
MEMBERSHIP

Since its inception in 2005, National CyberWatch has measured some of its success by the numbers of academic institutions, businesses, and government organizations in its membership database. Annual reports touted the increase in numbers of two-year and four-year member institutions, and the number of states in which National CyberWatch had representation. This year, those numbers have increased once again as follows:

- Current total number of members: 439
- Number of community college (institutional) members: 127
- Number of states with community college (institutional) memberships: 40
- Number of university (institutional) members: 99
- Number of states with university (institutional) memberships: 37
- Number of private industry members: 66
- Number of government agency members: 17
- Number of public industry and other academic members: 11
- Number of new members from January 2016 – December 31, 2016: 38 (23 community colleges; 15 universities)

National CyberWatch will be rolling out a new Membership program in 2017 with a focus on continuing to grow and provide benefits to our academic member network, while implementing a new program for individuals and corporations.

MEMBERSHIP BY THE NUMBERS: **2005-2017**



2016 COMMUNITY COLLEGE **CYBER SUMMIT**

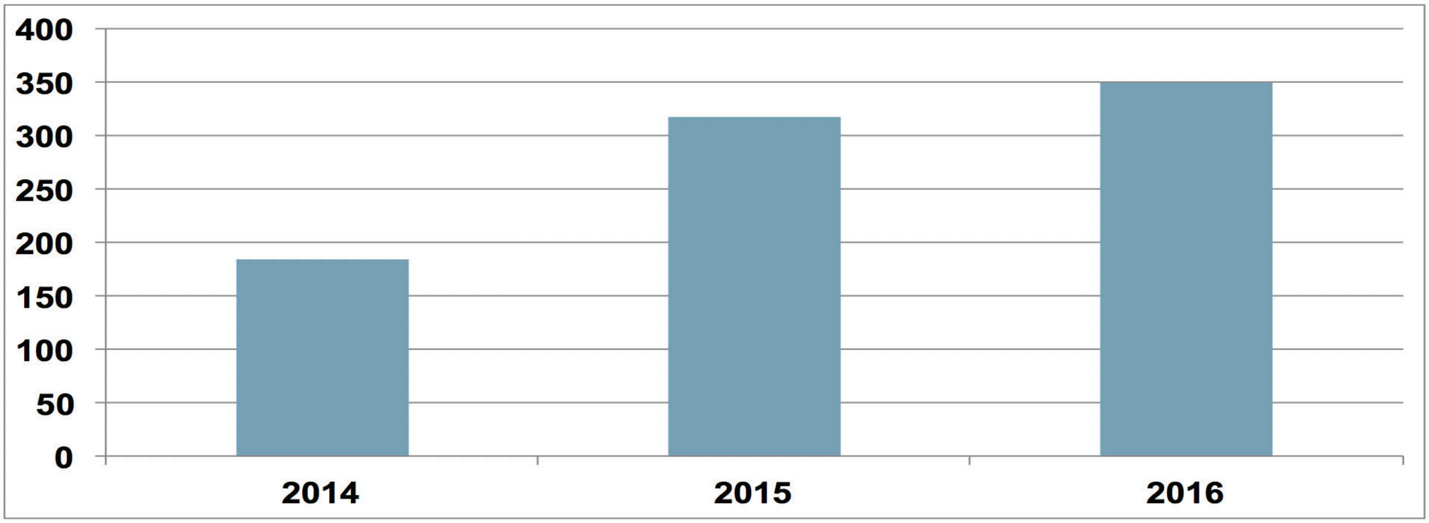
The Community College Cyber Summit (3CS) meets the need for a national academic conference that focuses on cybersecurity education at the community college level.

The third annual 3CS was held July 22-24 at the Community College of Allegheny County in Pittsburgh, PA. 350+ faculty, industry, and government participants attended keynote presentations and hands-on workshops focused on the Summit's theme: *Expanding the Boundaries of Cybersecurity Programs at Community Colleges.*

The 2017 3CS will take place June 28-30, 2017 at Prince George's Community College and National Harbor, MD. This year's theme is *Strengthening our Cyber IQ*.

> *"A great place to find, share, and explore curriculum and information for cybersecurity education."*
>
> **- Hal Casey**

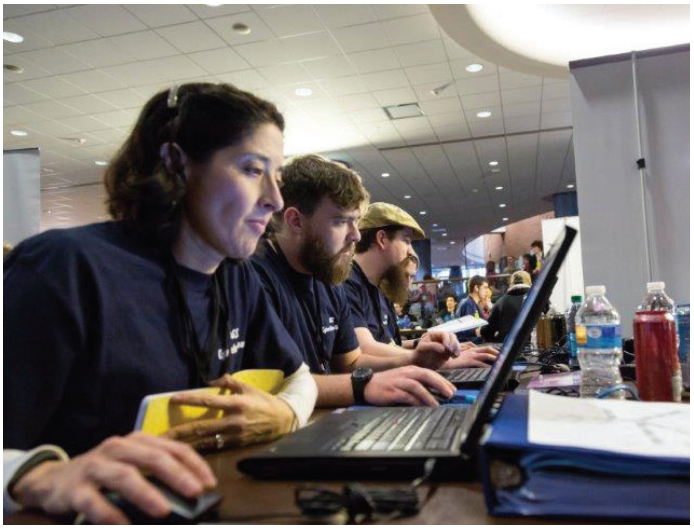
3CS BY THE NUMBERS: **TOTAL NUMBER OF ATTENDEES 2014-2016**



CYBERSECURITY **COMPETITIONS**

National CyberWatch continues to develop and run world-class cybersecurity competitions, which provide hands-on application of Information Security skills to enhance students' understanding of both theory and practice. In addition, these events are designed to offer engaging, entertaining, measurable, and scalable methods of learning to enlist a new generation of cybersecurity professionals, which is accomplished in the following ways:

- Providing inclusive individual and team competitive e-Sport experiences
- Creating a fun, experiential learning opportunity where players demonstrate skills/knowledge sets
- Promoting proficiency of specific cyber skills
- Preparing teams for other cybersecurity exercises
- Continuing the acquisition of skills tied to curriculum, industry needs, and professional certifications
- Enriching the classroom/training learning experience
- Promoting industry participation
- Addressing the lack of qualified cybersecurity professionals nationally
- Aligning competition events to academic calendars (e.g., semesters)
- Providing a mechanism by which participants can assess the effectiveness of their curriculum/training



MID-ATLANTIC COLLEGIATE
CYBER DEFENSE COMPETITION

Initiated by National CyberWatch in 2006, the MACCDC consists of both virtual qualifying rounds and a face-to-face Regional Finals round engaging full-time undergraduate and graduate degree-seeking students, representing four-year universities and community colleges from Delaware, the District of Columbia, Maryland, New Jersey, North Carolina, Pennsylvania, Virginia, and West Virginia. In the past 12 years, over 2,000 students have participated in the MACCDC.

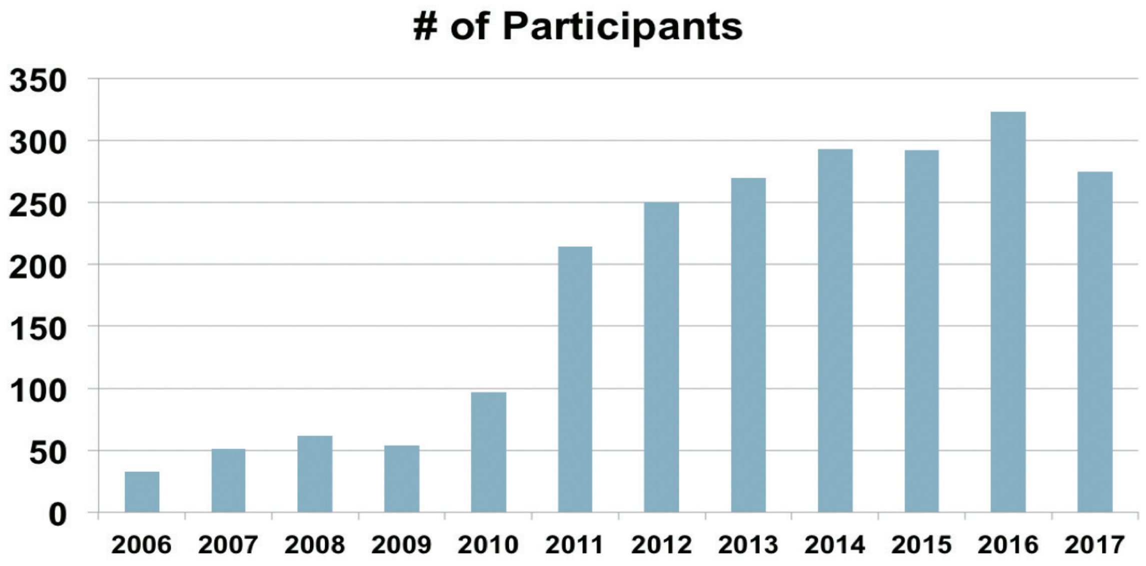
MA CCDC Mid-Atlantic Collegiate Cyber Defense Competition

The 11th MACCDC Regional Finals was held March 31-April 2, 2016 at the Johns Hopkins University Applied Physics Lab in Laurel, Maryland. Teams competed in Operation Cyber Bailout. The student teams managed and secured a financial system that came under attack by cyber terrorists. The terrorists represented a rogue nation state actor dedicated to bringing down the fictitious country of Hackistan's financial system. It was up to the eight student teams to manage and secure their systems in order to restore order to Hackistan's economy.

2016 Final Regional Team Standings:

1. Liberty University, VA
2. University of Maryland, College Park, MD
3. Towson University, MD
4. University of Maryland, Baltimore County, MD
5. Bloomsburg University, PA
6. Radford University, VA
7. Capitol Technology University, MD

The MACCDC continues to be one of the premier events of its kind in the country, as demonstrated by the continued growth and interest from its varied participants, volunteers, and sponsors.



2016 NATIONAL CYBER LEAGUE
FALL SEASON

Now in its sixth year, the NCL has a powerful and proven model - provide an ongoing virtual training ground for faculty and students to develop and validate cybersecurity skills using content aligned with individual and team games - which is scalable across many industry certifications, curricula, job roles, and verticals.

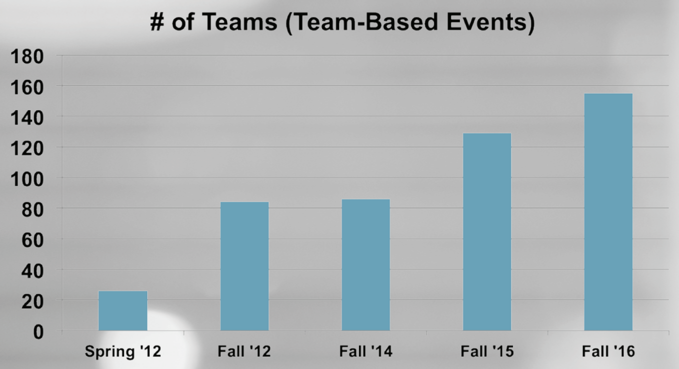
The NCL differentiates itself in the following ways:

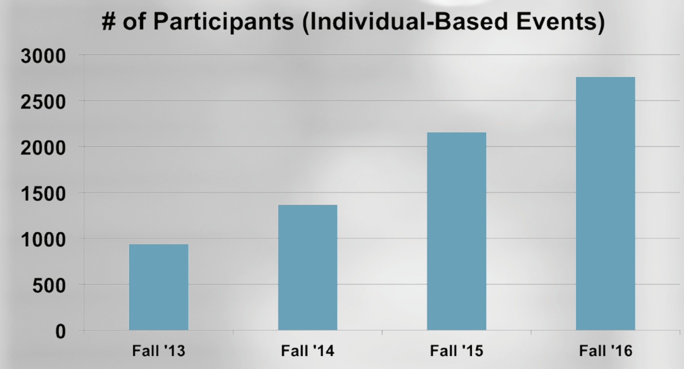
- Providing year-round knowledge and skills development and validation
- Integrating learning objectives in all activities
- Validating skills
- Reporting on individual's and team's game performance
- Scaling the numbers of participants/teams and learning/game environments

The 2016 Fall Season was by far the largest event the NCL has run and included:

- Record numbers of participants (2,760)
- Continued corporate sponsor (Facebook)
- Continued successful communications and marketing efforts
- Virtual preparatory lab exercises, enabling players to develop knowledge and hands-on skills any place, any time
- Mandatory Preseason game assessment to identify players with similar knowledge and skill levels
- Regular Season with two games optimized for individuals
- Postseason game optimized for teams
- Provided students with diverse skill levels, fun, and engaging learning and playing environments available anywhere, any time
- Measured how players perform in the games and produced individualized Scouting Reports (performance-based assessments)
- Gave faculty opportunities to enrich classes by integrating lab exercises and competitions into existing security-related curricula
- Stimulated individual cybersecurity skills development
- Created school pride for players and coaches

> *"This is a great place for my cybersecurity students to put into practice what we're teaching in the classroom. Whether you have years of experience or just starting out in the field, there is a wide range of events to challenge you and test your skills. I highly recommend NCL."*
>
> \- Alan W





"From all of us at Honolulu Community College, we wanted to sincerely thank you, your team, and Cyber Skyline for hosting and putting on the National Cyber League. The experience and lessons learned from these series of events have been highly beneficial for all of our students -- both from a technical and a motivational standpoint. It is my firm belief that all of our participating students have garnered a higher degree of aptitude within our field, regardless of what career path they will choose. We look forward to nurturing future teams and hope that you all continue to put on such an excellent and exciting event."

Jayson Hayworth
Vice President
HATS: Hawai'i Advanced Technology Society

NATIONAL **CURRICULUM**

When the National CyberWatch Center started in 2005, quality Information Security curriculum was in short supply, so the development of new curriculum was a necessity. In 2006, the National CyberWatch Center, working in conjunction with Anne Arundel Community College, MD, developed model Information Assurance and Computer Forensics curricula, which supported the growth of cybersecurity education nationally, including complete courses for degrees and multiple certificates.

National CyberWatch continues to promote its reference curriculum degrees and certificate programs in Cyber Defense, Network Security Administration, Network Forensics, Secure Software Development, and Systems Security Administration (**http://www.nationalcyberwatch.org/programs-resources/curriculum**), as well as work with academic institutions to implement new programs, or update existing ones.

In the coming months, National CyberWatch will be launching the following new reference degree and certificate programs:

- Cybersecurity Foundations Certificate
- Applied Associate of Science (A.A.S.) in Secure Software Development (with associated Certificate)

NSA & DHS NATIONAL CENTERS OF **ACADEMIC EXCELLENCE IN CYBER DEFENSE (CAE-CD) LEADERSHIP**

National CyberWatch continues to lead and expand its comprehensive support and technical assistance system for institutions who are new to the CAE-CD program, or that need to re-designate. National CyberWatch's demonstrated and continued leadership role in the CAE-CD program continues to impact the broader academic community and the students they serve by:

- Ensuring the CAE-CD program requirements continue to be the standard for truly excellent Information Security academic programs
- Improving the quality of the CAE-CD applications
- Disseminating timely and accurate information via the National CyberWatch Center's Digital Press and Webinar Series
- Articulating the CAE-CD value proposition to prospective schools, as well as presidents and senior leadership at two- and four-year schools

NATIONAL CYBERSECURITY STUDENT ASSOCIATION **LAUNCH**

The National Cybersecurity Student Association - **www.cyberstudents.org** - is a one-stop-shop to enhance the educational and professional development of cybersecurity students through activities, networking, and collaboration with their peers. This group supports the cybersecurity educational programs of academic institutions, inspires career awareness and encourages creative efforts to increase the number of underrepresented populations in the field.

Since its launch in April 2017, focus has been on building industry and professional association partnerships and growing the number of student members/Chapters.

RESEARCH

National CyberWatch research efforts are focused on documenting, promoting, and advancing evidence-based cybersecurity education and workforce development strategies and practices. Sample research questions include:

- What does Labor Market Demand Research reveal about the need for middle-skill cybersecurity positions and the ability of community colleges to respond?
- What are the features of the most successful transfer pathway models?
- Which cybersecurity competition design elements (e.g., scoring, mapping to learning objectives) are most effective at engaging students?
- What is the efficacy of the specific consortia that National CyberWatch has helped to form? Have these consortia resulted in more cybersecurity students, faculty, and degree programs? Are industry needs better aligned with academic programs?
- What factors influence engagement and self-efficacy development in simulation-based learning?
- What are the methods for quantifying and determining individual or team positioning on a learning curve?

ASSESSMENT

Assessment is a growing part of the National CyberWatch portfolio and one that promises new revenue streams and the possibilities of defining new markets. Some of the challenges in the assessment domain as it relates to cybersecurity include:

- Moving beyond a singular focus on knowledge
- Demonstrating the tangible impact of decisions and actions to effective performance
- Demonstrating which skills made the difference
- Demonstrating new approaches to testing to improve prediction
- Demonstrating new approaches to learning to improve knowledge
- Demonstrating new approaches to practice using simulation to improve skill
- Demonstrating new approaches to technology design to lower skill requirements for effective performance

LOOKING **FORWARD**

National CyberWatch will expand and enhance the Center's strategic and leadership roles in the following ways:

- Practice-Based Education solutions to the cybersecurity workforce skills crisis that combines work practice analysis, problem-based classroom or virtual instruction, and adaptive personalized simulation and serious gaming technology
- Accelerated learning programs integrating validated assessments, instruction, practice labs, and challenge scenarios to improve cybersecurity talent management in organizations
- Rapid deployment of customizable and adaptive curriculum that raises learner capability maturity in foundational cybersecurity concepts, principles, and practices
- Formative credentialing solutions that increase the number of capable cybersecurity professionals
- Formative assessments that provide valuable pedagogical resources to cybersecurity instructors to raise learner competency levels towards mastery in foundational course domains

SUMMARY

National CyberWatch promises continued and significant results, as well as far-reaching impact on cybersecurity education, workforce development, research, and assessment. National CyberWatch's track record demonstrates its capacity to elevate cybersecurity education and workforce development to the next level, and in doing so, fulfill on its mission of leading collaborative efforts to advance cybersecurity education and strengthen the national cybersecurity workforce. National CyberWatch's world-class team, academic member network, and industry and government partners, provide the necessary ingredients for success.

NATIONAL CYBERWATCH CENTER **TEAM**

The NCC team has benefited from continuity in leadership and knowledge transfer over the past 10 years, as well as from recruiting new subject matter experts from across the country bringing an infusion of new energy and varied perspectives. The 2016 NCC Team includes:

Casey O'Brien
Executive Director & Principal Investigator
Prince George's Community College
Maryland

Dr. David Tobey
Director, Research & Assessment
Co-Principal Investigator
Indiana University South Bend
Indiana

Dr. Margaret Leary
Director, Curriculum
Co-Principal Investigator
Northern Virginia Community College
Virginia

Dr. Vera Zdravkovich
Senior Advisor
Prince George's Community College
Maryland

Dr. Bob Spear
Senior Advisor
Director, Community College Cyber Summit
Prince George's Community College
Maryland

Lewis Lightner
Director, Operations & Programs
Competition Director, MACCDC
BrightPath Technology
North Carolina

Dr. Costis Toregas
Senior Advisor
Director, Scholarship for Service Four-Year
George Washington University
Washington, D.C

Fran Melvin
Director, Finance
Center Manager
Prince George's Community College
Maryland

John Sener
External Evaluator
Sener Knowledge
Maryland

Dr. Barbara Belón
Director, Member Services
Director, Scholarship for Service Two-Year
Belón Research & Practice
Pennsylvania

Anita Shelton
Administrative Associate
Prince George's Community College
Maryland

Lynn Dohm
Director
Marketing & Communications
Nelly Group
Illinois

Michael Burt
Virtual Lab Manager
Prince George's Community College
Maryland

NATIONAL **VISITING COMMITTEE**

The NVC, appointed by the NSF, provides informed feedback to the National CyberWatch team so it can improve its efforts. It also provides feedback to NSF in the form of a report, to help NSF evaluate National CyberWatch's performance and benefit from the NVC's perspectives on how the Center might improve its impact. The NVC also assists the Center's efforts by helping to get the word out about its initiatives and programs. The NVC meets annually and reports directly to NSF.

Nicholas M. Cefaratti
Information Security Systems Engineer
Harris Corporation
Florida

Dr. Philip Crager
Professor and Principal Investigator
Advanced Cyberforensics Education (ACE)
Consortium
Daytona State College
Florida

Dr. Gaby Hawat
NVC Chair
Senior Vice President
Operations and Global Initiatives
Florida Institute of Technology
Florida

Dr. Corby Hovis
Lead Program Director
Directorate for Education and Human Resources
National Science Foundation
Virginia

Dr. Victor Piotrowski
Lead Program Director
CyberCorps®: Scholarship for Service (SFS)
Division of Graduate Education
National Science Foundation
Virginia

Corrinne Sande
Director & Principal Investigator
CyberWatch West
Whatcom Community College
Washington

Elayne Starkey
Chief Security Officer
State of Delaware
Delaware

Georgia Weidman
Founder and CTO
Shevirah Inc.
Virginia

This material is based on work supported by the National Science Foundation (NSF) under Grant Number DUE-1204533 and DUE-1601150. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect those of NSF.

NATIONAL CYBERWATCH CENTER

www.nationalcyberwatch.org

Transforming lives.

PRINCE GEORGE'S COMMUNITY COLLEGE

www.pgcc.edu

www.nsf.gov