NISTIR 8287

A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce

Danielle Santos
Sanjay Goel
John Costanzo
Debbie Sagen
Patty Buddelmeyer

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8287

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8287

A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce

Danielle Santos
Applied Cybersecurity Division
Information Technology Laboratory

Debbie Sagen
Pikes Peak Community College
Colorado Springs, CO

Sanjay Goel
Dept. of Info. Security & Digital Forensics
University at Albany, SUNY
Albany, NY

Patty Buddelmeyer
Southwestern Ohio Council
for Higher Education
Dayton, OH

John Costanzo
Virginia Cyber Alliance and HRCyber Alliance
Old Dominion University
Norfolk, VA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8287

February 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8287
32 pages (February 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8287

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-0003
Email: nice.nist@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

Abstract

In September 2016, the National Initiative for Cybersecurity Education, led by the National Institute of Standards and Technology in the U.S. Department of Commerce, awarded funding for five pilot programs for Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development. The document that follows provides a summary of the five pilot programs and outlines a roadmap for building similar programs based on the best practices found and lessons learned.

The roadmap for successful alliances to build the cybersecurity workforce requires four primary components: 1) establishing program goals and metrics, 2) developing strategies and tactics, 3) measuring impact and results, and 4) sustaining the effort. Each section of the roadmap provides specific examples and activities that the pilot programs found to be successful and repeatable in other efforts.

Keywords

alliance; collaboration; cybersecurity; education; partnership; RAMPS; stakeholder; workforce.

Supplemental Content

RAMPS Web Page with additional information on the five projects: https://www.nist.gov/itl/applied-cybersecurity/nice/regional-alliances-and-multistakeholder-partnerships-stimulate-ramps

Acknowledgments

The authors would like to thank Cassie Barlow and Sean Creighton of the Southwestern Ohio Council for Higher Education and Tina Slankas of the Cyber Security Canyon for their contributions to this document. The authors also thank those contributors who reviewed drafts of this document: Marian Merritt, Rodney Petersen, Davina Pruitt-Mentle, Kevin Stine, Shannan Williams, Donna Dodson, Jim St. Pierre, and Jeff Marron.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

Table of Contents

List of Appendices

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

1 Introduction

The cybersecurity workforce shortfall is well documented. According to CyberSeek.org[1], there were 313 735 open cybersecurity-related positions from September 2017 through August 2018. The 2017 Global Information Security Workforce Study states that 1.8 million more cybersecurity professionals will be needed to accommodate the predicted global shortfall by 2022 [1]. The National Initiative for Cybersecurity Education (NICE) is addressing this critical issue by energizing and promoting a robust network and ecosystem of cybersecurity education, training, and workforce development. Supporting this mission, objective 3.3 of the NICE Strategic Plan emphasizes guiding career development and workforce planning by facilitating state and regional consortia to identify cybersecurity pathways addressing local workforce needs [2].

By fostering regional alliances:

- workforce needs of local business and non-profit organizations are better aligned with the learning objectives of education and training providers conforming to the NICE Cybersecurity Workforce Framework,
- the pipeline of students pursuing cybersecurity careers is enlarged,
- more Americans are upskilled and moved into middle-class jobs in cybersecurity, and
- local economic development to stimulate job growth is supported.

1.1 Background

In September 2016, NICE, led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, awarded funding for five pilot programs for Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development. These programs focused on bringing together employers who have cybersecurity skill shortages with educators to focus on developing a skilled workforce to meet industry needs within local or regional economies. Awards were provided to universities, a consortium, and a community college who pre-identified partnerships with at least one of each of the following:

- K-12 school or Local Education Agency
- Institution of higher education or college/university system
- Local employer

Each of the five programs had unique approaches to addressing the cybersecurity workforce needs in their region. These efforts included building interest in and pathways to become a cybersecurity professional. Programs also focused on encouraging more employer engagement in local communities in order to influence education and training providers to develop job-driven

[1] CyberSeek.org is an online tool that provides detailed, actionable data about supply and demand in the U.S. cybersecurity job market.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

training that provides the skills that businesses need. Brief descriptions[2] of each program are as follows:

Arizona Statewide Cyber Workforce Consortium
State of Arizona Region; based in Phoenix, Arizona
ArizonaCyber.org

The Arizona Statewide Cyber Workforce Consortium, led by Chicanos Por La Causa and Cyber Security Canyon, developed a unified approach to creating cybersecurity resources from a number of existing efforts. The partnership was used to provide a unity of vision, bridging traditional and non-traditional educational pathways to create cybersecurity talent. It also enabled the alignment of employers' efforts through the Greater Phoenix Chamber of Commerce Foundation. Assistance was provided to help align job descriptions to the NICE Cybersecurity Workforce Framework, review curriculum for greater relevance that adheres to program requirements of the National Security Agency and Department of Homeland Security designated two-year National Centers of Academic Excellence programs, and create job experiences for students interested in learning more about the field of cybersecurity. The partnership connected applicants from traditional and nontraditional backgrounds to employers to provide skilled workers for the growing number of cybersecurity positions in state government and the region's critical infrastructure segments, including manufacturing, health care, and the defense industrial base.

Cincinnati-Dayton Cyber Corridor (Cin-Day Cyber)
Southwestern Ohio Region, including Northern Kentucky; based in Dayton, Ohio
cindaycyber.org
Cin-Day Cyber RAMPS Final Report

Led by the Southwestern Ohio Council for Higher Education (SOCHE), Cin-Day Cyber focused on strengthening cybersecurity education to support the growth of a highly-skilled cybersecurity workforce. Working closely with secondary schools, higher education, industry, and government, Cin-Day Cyber researched local current and future job demand, developed and delivered workshops to build career interest in cybersecurity, created and managed cyber-related internships, and facilitated industry and higher education roundtables to develop partnerships that addressed the challenges of the cybersecurity workforce supply and demand in the Cincinnati-Dayton region.

Cyber Prep Program
Southern Colorado Region; based in Colorado Springs, Colorado
ppcc.edu/cyberprep
Cyber Prep Program RAMPS Final Report

The Cyber Prep Program at Pikes Peak Community College established a formal, sustainable

[2] In-depth program outcomes can be found in each of the programs' final reports. An overview of highlighted activities, sorted by topic area, can be found in Appendix B.

partnership between secondary-school districts, employers, and the college. The program built cybersecurity workforce development pathways to address local workforce needs and supported the development of cybersecurity programs in area high schools and in the college's area vocational program. The program created a summer cybersecurity work experience for high school students and provided opportunities for registered apprenticeships to ensure a sustainable cybersecurity workforce for the future.

It is demonstrated through data collected from each of these programs that regional alliances have a positive effect on educational and workforce pathways. Many examples can be provided to support this, including university and community college articulation agreements that helped save students approximately 50 credit hours or 1.5 years of study, internship partnerships that helped place over 100 students with local employers, and several workshops, trainings, career fairs, camps, and forums held. These activities build bridges between higher education and employers looking for current and future employees in cybersecurity.

Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance
Southeast Virginia Region, including Hampton Roads and Tidewater Regions; based in Norfolk, Virginia
securitybehavior.com/hrcyber
HR Cyber RAMPS Final Report

Old Dominion University's Center for Cybersecurity Education and Research coordinated the Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber). HRCyber is a partnership of educational institutions, government agencies, non-profit organizations, and private employers focused on developing educational pathways from high school through community college to four-year institutions and continued professional development, providing a capable and fully trained cybersecurity workforce for the region. The specific goal of supporting local economic development and job growth was achieved by aligning regional educational and skills development offerings to the workforce practices and activities of business and non-profit organizations within the Hampton Roads region.

Partnership to Advance Cybersecurity Education and Training
Capital District and New York City Region; based in Albany, New York
albany.edu/facets
Partnership to Advance Cybersecurity Education and Training Final Report

The Partnership to Advance Cybersecurity Education and Training was led by the State University of New York at Albany. New York's Capital Region has a unique workforce potential, with its range of higher education institutions and Science, Technology, Engineering, and Math (STEM) graduates and a growing advanced technology sector. The project built clear educational paths and increased regional workforce capacity for a range of potential careers in cybersecurity based on industry needs.

1.2 Purpose and Scope of Document

As a result of the outcomes and accomplishments of the RAMPS pilot programs, this document

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

provides a record of the methods and best practices used and presents a roadmap for communities interested in building similar regional alliances. It describes the essential components of a successful alliance and provides examples of activities that can be accomplished by having such partnerships.

This publication was created for those seeking guidance on how to organize and facilitate regional efforts to enhance cybersecurity education and workforce development. While this document explores some elements for consideration when forming alliances, it is not intended to be a how-to guide that gives specific instructions. NIST believes that this is best left to the local or regional experts who are familiar with the needs of their specific community.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

2 Key Challenges and Strategies to Address Them

There is no shortage of challenges when it comes to building a better cybersecurity workforce, and challenges will vary from region to region depending on the maturity of existing efforts. Awareness of these challenges will aid in forming strategies and priority actions for regional efforts. The topics that follow are key challenges that the RAMPS pilots encountered in building their programs.

1. Employers are unsure about their cybersecurity workforce needs.
2. There is a disconnect between workforce supply and demand in the context of talent.
3. Resources for education and workforce development programs are independent rather than coordinated.
4. Retention of talent in small communities is often difficult.

2.1 Determining Workforce Needs

With the exception of companies that provide cybersecurity products and services, most employers commonly do not understand their own cybersecurity workforce needs, including the number of professionals needed or the cybersecurity skillsets they should hold. Companies continue to struggle with recognizing a return on their security investments, especially since gains are often seen as the absence of attacks and senior managers typically operate from a reactive stance, often failing to understand their own proactive, ongoing security needs.

In response to this challenge, several RAMPS groups conducted regional surveys to determine current and future workforce needs by measuring and assessing the knowledge and skills of cybersecurity new hires. Surveys were conducted amongst employers, trade associations, and academic institutions [3][4]. The outcomes of these surveys ranged from providing baselines that were used to help academic institutions in revising curricula and determining the need for new academic programs to the development or expansion of internship opportunities. Further, some communities created programs that train executives on the business needs and challenges of cybersecurity so that management decisions can be made in pace with evolving technologies and cybersecurity risks.

2.2 Connecting Workforce Supply and Demand

The second challenge is the mismatch between workforce supply and demand. While there are many emerging academic programs in cybersecurity, there is a mismatch between the needs of employers and the students coming from these cybersecurity degree or certificate programs[3]. This skills gap is driven partly from the rapid changes occurring in cybersecurity that lag behind educational programs in colleges and universities.

RAMPS pilot communities addressed this challenge by holding a variety of workshops. Some sessions brought together industry representatives and curriculum designers to create and refine course curriculum content that would better meet industry needs. Feedback from industry during these workshops led faculty to require internships for cybersecurity students so that they would gain valuable work experience before graduation.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

Progress was also made by developing more technically-focused two-year programs at community colleges that can be linked to bachelor's degree programs at four-year schools. These programs can meet local talent needs for information technology professionals with deep cybersecurity knowledge. Curriculum updates can be approved more quickly and graduates are work-ready sooner because community colleges are required to be responsive to employer demand. Interdisciplinary programs in cybersecurity were also developed. In one case, a cybersecurity major and minor was built with courses drawn from multiple disciplines such as philosophy, computer science, computer engineering, information technology, and criminal justice.

Another successful method used to connect supply with demand was to collect and analyze data to understand cybersecurity workforce needs and opportunities. This included: 1) conducting educational program inventory and gap analyses; 2) creating an inventory of regional expertise in cybersecurity and cybersecurity research being conducted at area universities; 3) analyzing open cybersecurity positions to determine the scope of positions at entry-, mid-, and senior-levels; and 4) analyzing cybersecurity policy and practices in the region.

2.3 Creating Synergy Amongst Existing Programs

The third challenge is limited and constrained resources. While there is good financial support available, it is frequently expended over significant numbers of educational programs, some of which may be redundant. Consequently, some organizations are unable to fully develop educational and training programs with the programmatic depth required to adequately prepare learners for the workforce. Other organizations that are able to establish high-quality curriculum may not be able to maintain them, including through virtual or physical labs and facilities. Resources should be synergized and focused to minimize redundancy and improve program quality.

Leveraging existing consortia helped the RAMPS pilots address this challenge. In one case, partnering with the National Centers of Academic Excellence in Cybersecurity (CAE) program allowed regional colleges and universities to become an attractor for students seeking to enroll in institutions with the CAE designation. The CAE program recognizes colleges and universities with cybersecurity programs that have met stringent criteria. It has designations in Cyber Operations and Cyber Defense. In another case, local and state-wide committees were utilized for creating partnerships.

Taking advantage of modern technologies can also help to solve this challenge. For example, virtual labs and cyber ranges proved to be a successful method of minimizing resources needed to achieve maximum reach. Linking cybersecurity lab environments within a region can allow for greater, more seamless collaboration.

2.4 Retaining Talent

The fourth challenge is the flight of top cybersecurity talent from smaller markets to larger markets that offer higher salaries. Small and rural economies continue to struggle to attract and retain cybersecurity talent, especially since they are less likely to be competitive with market salaries for cybersecurity professionals in larger markets. To facilitate economic development, innovative methods can be used to retain local talent.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

This challenge can be addressed by seeking out and collaborating with business leaders who understand the value of retaining workers in a specific region and who are willing and able to work with the business development community, academic institutions, and other businesses to build the locality's cybersecurity ecosystem. Organizing meetings can be helpful in bringing these diverse groups together to discuss ways to attract and retain additional workers and cybersecurity businesses into the region.

A cybersecurity internship or apprenticeship program is another way to help develop home-grown cybersecurity talent and retain those workers locally. These programs allow students to work with local companies and provide networking opportunities with professionals in the career field. These connections often lead to full-time employment for the interns or apprentices.

Additionally, small and rural economies should consider recruiting students nationally to participate in internship programs in their region. Visiting students can help further promote the region as a great place to work and live. Establish partnerships with chambers of commerce and other community advocates to welcome the students or new employees to the region by providing them the opportunity to participate in engaging regional activities.

The RAMPS program demonstrated that building an alliance of academia, industry, and government helped regions to address these challenges successfully. Developing such alliances requires resources, individual and organizational champions, supportive leadership, and perseverance. The effort may take time to develop as programs are built piece by piece; yet, collaboration to knit together existing programs can provide a jump start. Relationships with the right organizations must be nurtured by identifying mutual synergies then leveraging them to create a shared vision.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

3 Roadmap

The co-authors of and contributors to this document analyzed the outcomes of each of the five RAMPS pilot programs and have created a model by which similar programs can be created in other regions. This roadmap describes the steps that the pilots took in developing, maintaining, and measuring the success of their alliances.

One of the first actions that should be taken when starting a RAMPS-like program is to create a clear set of goals for the alliance, realizing that it will only be successful if each goal is well-defined and all participants are able to see the benefits it will produce. The second priority should be to develop and begin to implement strategies. Determine what mechanisms will be used to coordinate the alliance and what the primary activities of the alliance will be. The third action is to establish clear metrics and measurement techniques for each goal and tactic within the alliance's strategy to ensure that realistic expectations are set. With these underpinnings, the alliance can then launch, using the roadmap provided below as a guide:

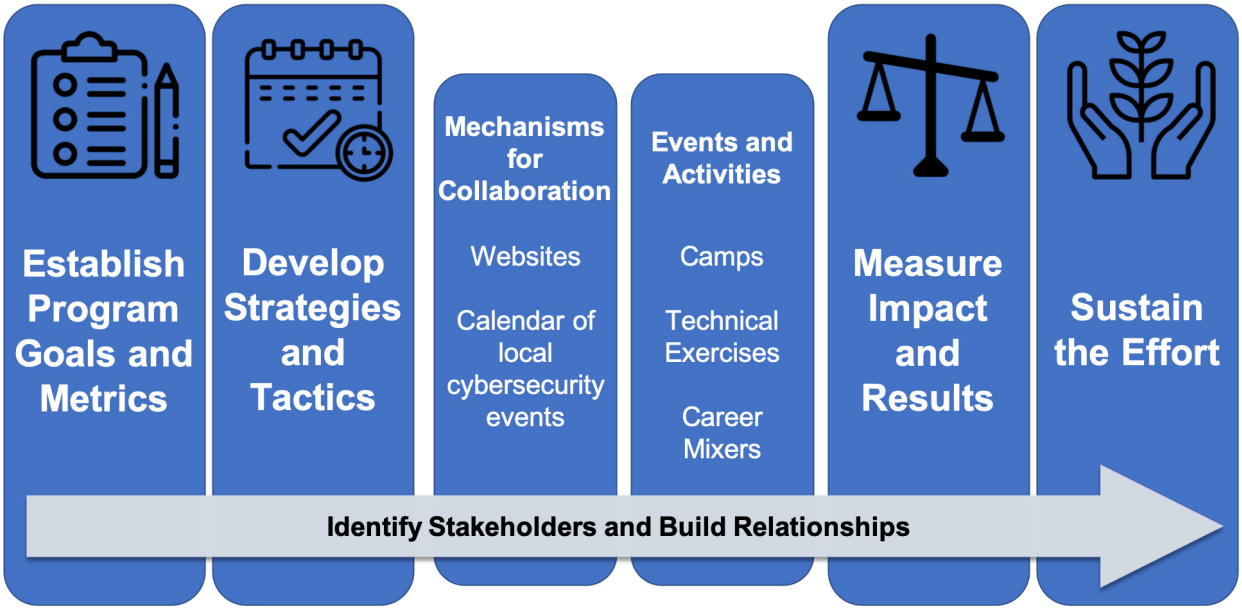

Figure 1 - RAMPS Roadmap Graphic

3.1 Getting Started

Start by identifying a lead organization that can be the catalyst to lead and keep the effort moving forward. Second, identify people willing to provide formal administrative support including scheduling, organizing, and documenting convenings and tracking progress. Consider having a project manager as part of the administrative team who can help to organize the project, manage workflow, coordinate meetings, and hold organizations accountable for their outcomes.

To determine the scope of a regional alliance there are many criteria for consideration. Regions can vary in size and range from specific cities to economic communities that cross state boundaries. Refer to section 1.1 for examples of regions from the RAMPS pilot programs.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

Consider the following when defining an alliance:

- Create meaningful relationships with individual companies by inviting them to join advisory boards or serve as subject matter experts on panels and working groups.
- Research relationships that will be complementary to your goals and priorities.
- Find anchor institutions and others who are already investing resources, including money or time, into similar efforts.
- Determine where the most impact can be made and opportunities for impact, including economically-depressed areas or low-income areas.
- Recognize statewide dynamics, drawing regional lines where it makes sense.
- Seek out opportunities for virtual collaborations while also assessing the ability to make face-to-face contact so that work can start, and relationships can be built.
- Size regions appropriately so that it is reasonable and can be manageable with available resources, keeping in mind that local or state government funding may be tied to keeping jobs in a specific geographical area.

3.2 Identifying Stakeholders

Including multiple types of stakeholders in your regional alliance will increase opportunities for success. It should be clear that the stakeholders of the alliance can vary across different regions. For instance, in areas near capital cities or military presences, government agencies, in their role as employers, can be strong partners. In other areas, industry could be the primary partner for such an alliance.

In addition to providing valuable insight and subject matter expertise, stakeholders may also have existing efforts that would benefit from participation in the alliance. Other groups may have tools, such as existing cyber ranges or established strategies or frameworks that can be utilized by the group. Finding synergies and identifying projects that can show early success to the community can help bring awareness and buy-in from the community.

Table 1 provides an idea of the types of groups to consider when building a cybersecurity education and workforce regional alliance.

Table 1 – Types of Stakeholders

Academia	Government	Industry	Other
Public and Private Primary and Secondary (K-12) Schools and Districts and Career Tech Centers	Local Government Business and Economic Development Offices	Local Small or Medium Sized Companies in Multiple Business Sectors (technology, health, energy, government services, financial, etc.)	Chambers of Commerce
School Boards	City and County Governments	Government Contractors	Regional Economic

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

Academia	Government	Industry	Other
			Development Organizations
Community Colleges	State Departments of Education	Professional Associations (InfraGard, ISACA, International Information System Security Certification Consortium , Information Systems Security Association, CompTIA, etc.)	Space Grant Consortiums
Public and Private Colleges and Universities, including Minority Serving Institutions and National Centers of Academic Excellence in Cybersecurity	Local and State Elected Officials including: Legislators, Governors, Caucuses, and Judges	Cybersecurity Companies Providing Products and Services to Other Organizations	Local Media
Other Academic Institutions (Trade Schools, Apprenticeship Programs, etc)	Federal Elected Officials (U.S. Representatives & Senators)		Non-profit Organizations (Trade Associations, Technology Councils)
Influential Community Leaders, including: Parents, School Counselors, Career Navigators, Teachers and Faculty, Academic Administrators, and School Boards	Federal Agencies such as the National Science Foundation, Department of Homeland Security and Secret Service, Federal Bureau of Investigation, and Department of Defense		Small Business Development Centers
	Federally Funded		

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

Academia	Government	Industry	Other
	Labs and Research and Development Centers		

3.3 Building Relationships

After core stakeholders are identified, it is critical to begin building and maintaining both formal and informal relationships among them. These relationships can lead to additional opportunities for research, funding, work, and other areas of common interest. Relationships can initially be built by interviewing each stakeholder formally, based on a set of structured questions to determine their organization's needs and wants, assets, and concerns. Next, holding a formal session to allow stakeholders to get to know one another can be useful, allowing the lead organization to report on existing synergies among the stakeholders, common concerns, and possible gap areas.

Once stakeholder contacts are established, it is critical to maintain the relationship. This can be done by holding quarterly or monthly meetings, roundtables, workshops, or conferences. Regular meetings keep the stakeholders engaged in the project, while periodic workshops and conferences allow the regional alliance to expand its reach by bringing in experts in specific topics and opening these events to the public.

3.4 Establishing Program Goals

As a prerequisite to forming alliances and developing a plan of action, it is important to perform an environmental scan of existing efforts to minimize unnecessary duplication of effort. While this activity will be ongoing, an initial assessment of efforts already in place and existing groups who may have a similar mission is beneficial.

Analyze existing supply of potential cybersecurity workers and how to move them into cybersecurity careers. Start by examining traditional technology fields – computer science and engineering – but also consider non-traditional disciplines as well as adults who can be reskilled to move into cybersecurity. For example, start by creating an inventory of existing information technology programs in area high schools, colleges and universities, and private training programs, looking for those that have a cybersecurity focus. Next, assess which organizations support extra-curricular activities such as CyberPatriot competition teams or GenCyber summer camps for students and teachers. Representatives from organizations that have existing programs or have begun to develop new programs can be recruited to join the core group of alliance stakeholders.

After assessing the landscape, create a vision for the collaboration. Consider the target stakeholder groups and the potential impact of the regional alliance and its ability to improve existing efforts and launch new initiatives. To be successful, leaders from the various stakeholder groups need to define scale, scope, and boundaries for the program. Often, a subgroup from the core team of stakeholders can develop a draft mission and vision, asking for input from the larger group before finalizing them. Completing this step early will allow stakeholders to buy in to the vision early, too, making it easier to align themselves with program priorities and activities and

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

recruit additional members to help.

3.4.1 Make a Realistic Plan

Begin by determining the purpose of the program – the "why." This will be unique to each regional alliance but should be agreed upon by all stakeholders involved. Examples of purpose can range from wanting to grow talent in specific categories of cybersecurity work to educating executives on why cybersecurity should be a priority for their organizations and how they can build their resiliency through a stronger cybersecurity workforce. A well-articulated purpose statement can help to rally additional employers, K-20 faculty and administrators, and non-profit leaders to work collaboratively to reach program goals.

3.4.2 Start the Documentation Processes

Having a well-documented plan will not only keep efforts focused but also serve as a reference point when reaching out to new stakeholders. Additionally, keeping record of progress and success can lead to potential funding and program expansion, often from outside the group's sphere of influence. Providing timelines in the plan will help keep alliance members organized and focused, especially as the effort grows. Publishing this information allows participants to speak with one voice about the purpose of the effort and its execution which helps to amplify the alliance's efforts. It also helps with celebrating progress as milestones will be well-known, and progress will be easy to monitor.

The RAMPS pilot programs had varying methods to document their strategic plans and progress made throughout the duration of their projects. Methods included the development of strategic plans and project plans, conducting regular meetings with stakeholders, and producing minutes and posting proceedings from workshops.

3.5 Developing Strategies and Tactics

There are many long and short-term activities that can be pursued which will vary depending on the mission, vision, and the available resources of your program. The RAMPS pilot programs identified common tactics that were beneficial to all projects; these are described below by way of mechanisms for collaboration and holding events and activities.

3.5.1 Establish Mechanisms for Collaboration

Focusing on external collaboration and information sharing, a website should be established to serve as a resource for partners and outreach to new community members. The website can be a landing place to share resources, links to career discovery tools, and a calendar of local cybersecurity events. It can also provide a space to share documentation of the alliance's progress and reports.

Internal collaboration, on the other hand, can be managed through project management platforms. There are free project management or collaboration tools available to consider or a stakeholder member of your alliance may have access to a tool that can be shared. Examples of tools used for the RAMPS pilots include GoogleDocs, GoogleSheets, and SharePoint.

3.5.2 Host Events and Activities

Holding events to introduce stakeholders to one another and give them baseline information to place them on equal footing is a great way to launch a new regional alliance. In the short term,

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

the RAMPS pilots found that it is significantly better for the program if events get started immediately, noting that the desire to achieve perfection can get in the way of getting started. Implementing smaller pilot events or iterations of an event or activity can be a good place to start and then continuously improved upon. Example activities include:

Technical Exercises Including Competitions and Ranges

- Cybersecurity Competitions or Challenges - learners use skills in networking, operating systems, and basic computer science concepts to defend a digital infrastructure. They often compete in teams and use virtual images to locate potential vulnerabilities and harden their system, all while maintaining critical services. Teams may also be required to participate in a written assessment of a company's cybersecurity needs as well as a proposal and bid for services to be provided. Examples include K-12 or collegiate competitions, challenges, capture the flags, Packet Wars, and Hack-a-thons.
- Cyber Ranges - virtual labs and simulations that help train learners. Examples include the Arizona Cyber Warfare Range, HRCyber Cyber Lab Collaborative, Old Dominion University/Tidewater Community College/Thomas Nelson Community College cyber virtual lab partnerships, and The University at Albany/New York State Information Technology Services Cyber Range.

Informational

- Industry Day - invite employers to learn more about the region's cybersecurity education initiatives, learn how to "plug in" and assist, and network with area faculty and administrators.
- Exhibit Booth - seek out industry stakeholders at established events or conferences to find a champion of the company and encourage employers to provide experiential learning if they want to hire experienced candidates.
- Student and Parent Events - hold events such as Cyber Saturdays for students to work with cybersecurity experts from both industry and academia while their parents are given information on the potential career opportunities in cybersecurity.
- Presentations - provide career awareness materials to learners. Materials from the National Cybersecurity Career Awareness Week Toolkit can be downloaded and adjusted so that they are tailored to your audience.
- Workshops - coordinate or participate in meetings to engage in intensive discussion and collaboration with stakeholders. Examples include Developing the Curriculum (DACUM) workshop and strategic planning workshops.
- Symposiums and Conferences - host, speak at, or network at cybersecurity conferences. Conferences can be geared toward information sharing and collaboration, training, or a mix.

Educational

- Camps - host, participate in, create lesson plans for, promote, or volunteer at camps such as Cyber Warrior Princess, GenCyber, CyberPatriot, or youth coding camps that are based on using the Raspberry Pi.
- High School and College Internships - help connect students with employers to provide them with internship opportunities and assist companies in developing internship programs.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

- Executive Forums and Trainings - offer forums for executives to share cybersecurity concerns and provide trainings to inform senior leaders on the importance of a strong cybersecurity workforce. Executive awareness programs should focus on basic cybersecurity awareness so that executives feel empowered to make proactive investments in cybersecurity. The education should be case-driven, addressing specific tasks that executives need for cybersecurity management in their organizations.
- Scholarships - seek out government funding or sponsorships from industry to provide financial assistance to students pursuing education in cybersecurity or related programs.

Networking

- Internship Fairs - host or encourage students to participate in in-person or virtual fairs to meet with employers and explore opportunities for employment through internships.
- Career Mixers - host or encourage students to participate in activities to help prepare them for the workforce and facilitate opportunities to meet with employers, such as mock interviews or resumé building workshops.
- Meetups - host, volunteer, or be a guest speaker at meetup events that convene interested parties to learn about cybersecurity topics.

Media and Marketing

- Web Presence - create a website where you can post notifications of upcoming events, share resources, and keep others informed of your work.
- Videos - create videos to promote cybersecurity education and career opportunities. Videos can include interviews with current practitioners to show what "a day in the life" looks like or provide data on the importance and impact of cybersecurity.
- Media Outlets - share your progress and accomplishments with news outlets and publishers to further boost your messaging.

3.6 Measuring Impact and Results

It is important to define metrics that will be used to measure the impact and results of the regional alliance. These metrics should be clearly defined and integrated into the plan early and updated along with all other documentation about the regional alliance's efforts. Metrics may vary depending on the type, size, mission, and goals of the alliance. Example metrics used by the RAMPS pilots include:

Environmental Scan Metrics

- Company surveys of employees and managers
- Number of students not able to be placed in employment
- Number of unfilled, available jobs in cybersecurity
- Number of educational programs offered and the number of students completing each program

Relationship Building/Stakeholder Metrics

- Number of executives that join the advisory board
- Amount of support from leadership via financial resources and advocacy

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

Events and Activities Metrics

- Attendance at community events
- Attendance for full events vs. part of the event
- Individual and team ranking in competitions

Media and Outreach Metrics

- View counts, comments, and shares on videos and other multimedia
- Visits, clicks, and other metrics for websites and posted materials
- Number of documents or digital artifacts produced and distribution numbers
- Number of media contact connections
- Number of press releases

Impact Metrics

- Number of industry partners or other meaningful relationships, new jobs, or companies created
- Stories that can be told about the results from and effects of the alliance – i.e., that show external validation, additional funding, promotion by others, etc.
- Level of economic return – for example, transfer pathway agreements saving students money and getting them into the workforce quicker
- Number of job seekers hired
- Number of new programs created
- Number of barriers removed – for example, helping underserved communities gain access to computers
- Number of new faculty
- Increased enrollment numbers

Other Metrics

- Number of formal internships created
- Measuring multi-purpose use for products, tools, or resources that were created
- Number of internships or apprenticeships completed
- Increase in community college crossover via articulation agreements and the expansion of the two-year to four-year pipeline
- Increase in high school programs, both academic and extra-curricular activities such as competition teams

Measurement of progress, impact, and results leads to evidence of maturity. Building a cybersecurity community involves integrating the entire ecosystem within a region, including the resources of educational institutions, industry, and state and federal governments to facilitate collaborations that support the community's entire spectrum of cybersecurity needs and workforce potential. The goals of such an ecosystem are: ensuring strong and community-relevant training, increased cybersecurity workforce capacity, facilitated learner placement, and fostered cybersecurity innovation. The process of building the ecosystem requires foundational efforts and careful planning as the program matures over time. Figure 2 highlights the different stages of maturity and benchmarked activities against which the maturity of a program can be gauged.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

Figure 2 - RAMPS Maturity Model

Level 1: Individual

- Individual faculty, researchers, or employees at non-profit organizations secure funding and work on projects
- Some training or formal education courses in cybersecurity, but no dedicated programs
- Volunteer practitioners serve as speakers or mentors for individual classes, clubs, meetups, or community meetings

Level 2: Programmatic

- Dedicated cybersecurity programs are established within K-12, graduate or undergraduate, and through training providers or employers
- Funded research programs
- Organized and recurring extra-curricular activities

Level 3: Institutional

- Dedicated champion at the institution or organization
- Commitment from upper management
- Institutional resources dedicated to cybersecurity education, research, and workforce development
- Accredited programs such as Career and Technical Student Organizations, National Centers of Academic Excellence in Cybersecurity, and participation in the Registered Apprenticeship Program
- Established hiring programs such as employer-led commitments or campaigns and involvement of University Career Services in student placement
- Established cybersecurity research centers

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

Level 4: Community

- Established community advisory board with diverse representation from academia, industry, and government
- On-going collaborations across multiple academic institutions, including K-20 and coordinated programs across multiple institutions (e.g. pipeline from community colleges to four-year colleges and universities)
- Growing public-private partnerships in research and training
- Dedicated cybersecurity job fairs
- Cybersecurity awareness for community via seminars and lectures for different demographic groups, learning pamphlets for different audiences, and basic functional cybersecurity classes for the community
- Academic programs coordinated with the community such as working with state agencies for retraining the workforce, working with corporations to provide courses on site, and developing high school programs that offer credit at colleges or universities
- Community involvement in cybersecurity events and academic programs such as business-sponsored public lectures
- Economic development programs to support innovation in cybersecurity
- Student placement pipeline into regional employers

Level 5: National

- National-level reputation and ranking of educational programs
- Research collaborations with universities across the country
- Engagement with federal agencies, including economic development funders
- Shared best practices for other communities to use and learn from
- Well-funded security research programs with large federal and state grants
- Student placement pipeline with national employers

3.7 Sustaining the Effort

The ultimate goal should be to create a self-sustaining effort that will continue to address the workforce development needs of the cybersecurity ecosystem within the region. Tapping into existing efforts and initiatives at the start of forming an alliance can enable progress in the long term to grow and gain momentum. Additionally, allowing participants maximum flexibility to define the alliance's goals and activities increases the likelihood that the initiatives will be sustainable. With buy-in from all participants, there is greater likelihood that specific projects and goals of the program will spin off into their own efforts.

It can be challenging to sustain a program with a mix of funding resources. Before you commit to accepting new funding sources, research and consider carefully all possible funding sources, including federal and state grants, private sector grants, and industry memberships. For example, the RAMPS pilot groups sought out research and workforce development grants and growth and opportunity funds from state and local governments. They applied for federal government funding opportunities from the National Science Foundation, Department of Labor, and others to gain additional funding to continue momentum.

4 Conclusions and Other Considerations

In conclusion, bringing together the multiple stakeholders in the cybersecurity ecosystem – industry, government, and educational institutions – can help communities address many of the cybersecurity workforce challenges that they face today. There are synergies among stakeholders that can be a natural glue for establishing a collaborative and local cybersecurity ecosystem. However, recognizing those synergies requires careful nurturing, relationship building, and patience. The challenge is to convince organizations to invest in collaboration as a business imperative and as a mutually beneficial and strengthening activity, not just as a charitable contribution.

This document provides a roadmap based upon models from the five RAMPS pilot projects from which regional alliances and partnerships can be formed to strengthen the cybersecurity workforce. It does not include an all-encompassing project plan but rather a starting place and important milestones.

Each RAMPS program was organized differently and had unique goals.

> Cin-Day Cyber created new synergies between individuals and companies that had not existed previously. The initiative enabled a deeper understanding of the cybersecurity industry and workforce needs and helped strengthen the alliance among industry, higher education, and K-12. Further, the work inspired numerous students to pursue careers in cybersecurity, established vital connections with industry, enhanced institutional collaboration, and provided critical research in cybersecurity for the region.
>
> The Cyber Prep initiative established a formal, sustainable partnership between school districts, employers, Pikes Peak Community College, and many local workforce development-related agencies and organizations. After thoughtfully assessing local assets and documenting gaps, the Cyber Prep team launched several new efforts to create or enhance programs for teens to explore cybersecurity. These efforts now bolster the region's larger cybersecurity ecosystem.
>
> HRCyber expanded the cybersecurity ecosystem within Hampton Roads (southeast Virginia) by linking stakeholders together who may not have otherwise connected and developed ways that these stakeholders could partner and collaborate in finding qualified candidates to fill the cybersecurity workforce needs across the region.
>
> At The University at Albany, the partners demonstrated that a strong cybersecurity regional alliance can be built (in the Capital District), and the academic program and students are reaping the benefits.

As shown through the diversity of the RAMPS pilots, there is no one right way to build a regional alliance. Merely having an organization play the convener role can help cybersecurity workforce development in a region, leading to national impact.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

References

[1] Frost & Sullivan (2017) *2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk.* https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx

[2] NICE Program Office (2016) *NICE Strategic Plan.* https://www.nist.gov/document/nicestrategicplan011218webpdf

[3] Social Science Research Center at Old Dominion University (2017) *Final Data Report*. http://securitybehavior.com/hrcyber/doc/2017_Final%20Data%20Report.pdf

[4] Pikes Peak Community College (2018) *Cybersecurity Education And Training Assessment: Assessing the Skills Gap in the Colorado Springs MSA*. Page 36 https://www.nist.gov/document/rampswesternregionfinalreportmay2019pdf

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

Appendix A—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

CAE	National Centers of Academic Excellence in Cybersecurity
Cin-Day Cyber	Cincinnati-Dayton Cyber Corridor
CTE	Career and Technical Education
CTSO	Career and Technical Student Organization
DACUM	Developing the Curriculum
HRCyber	Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
RAMPS	Regional Alliances and Multistakeholder Partnerships to Stimulate
SOCHE	Southwestern Ohio Council for Higher Education
STEM	Science, Technology, Engineering, and Math

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

Appendix B—Best Practices and Example Activities

This list provides examples and best practices used by the RAMPS Pilot programs. It is organized by five topic areas: Advising and Informing, Building Curriculum and Training Programs, Activities for Learners, Activities for Job Seekers, and Outreach.

Advising and Informing

1. Create a cybersecurity advisory board with top executives of organizations which can be instrumental in creating synergistic relationships with employers.
    a. The University at Albany created a very strong advisory board of senior organizational leadership which was instrumental in helping shape curriculum, organizing cybersecurity job fairs, providing direct recruitment of talent by employers, and building collaboration in funding opportunities. The advisory board also inspired several very talented cybersecurity professionals from local organizations to teach at the University at Albany and was beneficial in the development of relationships across multiple industries and academic institutions.
    b. Cin-Day Cyber established a Leadership Council that met monthly and included key partners in the alliance such as higher education, economic development, K-12, industry, and government. The group acted as a steering committee to inform events and initiatives, as well as served as ambassadors for cybersecurity across the state of Ohio in an effort to extend relationship building that resulted in additional support for cybersecurity education.
2. Bring together key faculty and administrators from across the educational spectrum to discuss what is taught at K-12, community colleges, and four-year institutions. This will assist in developing pathways into a cybersecurity career.
    a. Cin-Day Cyber used a previously established Degree Finder, modified it to add cybersecurity degrees and certificates, then promoted the tool to students, showing them a variety of opportunities and career paths in cybersecurity.
3. Connect with local employers
    a. Cyber Prep held annual Industry Day sessions, inviting employers to learn more about the region's cybersecurity education initiatives, learn how to "plug in" and assist, and network with area faculty and administrators.
    b. Cyber Prep helped companies develop paid summer internships for high school students and helped school districts recruit participants and place them with employers. In all, 31 high school students were placed at 17 different companies across two summers of the program. Assignments included work with defense contractors where officials had to make the case that teens under age 18 could contribute in meaningful ways. The program was so successful that some students continued their internships into the fall semester while others received offers to return to work in subsequent summers as they entered college. All employers were impressed with the level of talent, helping them to understand that hiring a local workforce is a viable option.
    c. Cin-Day Cyber connected 74 college students with paid internships in both the private and government sectors, to expose students to experiential learning opportunities.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

d. Cin-Day Cyber partnered with two regional and one state economic development agencies to attract summer interns and to develop campaign efforts to retain existing talent and attract new talent to the region.
e. HRCyber developed a high school cybersecurity internship program. In this internship, the students worked 30 hours with a local cyber company and they were paid $10/hour. A total of 20 students completed these internships; several were asked to stay on as an intern (paid by the employer) and one was offered a part-time position. These activities allowed the participants to learn from subject matter experts in cybersecurity from the local colleges/universities, federal government, and cybersecurity business professionals.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

Building Curriculum and Training Programs

1. Educational programs need to define a clear focus area, and then map their curriculum to reference standards such as those provided by NIST and NICE. This curricular alignment allows for common goals, terms, and understanding of skills in the field which are effective bridges between academia and industry. Consider using the Developing a Curriculum (DACUM) technique to assist in aligning the industry requirements with the academic courses and programs.
    a. HRCyber held a Developing the Curriculum (DACUM) workshop with a panel of industry representatives who spent two days identifying the knowledge, skills, and abilities of a cybersecurity analyst. This information was then used to create a DACUM chart that colleges and universities could use to create and refine course curriculum. As a result of this workshop, Old Dominion University changed the internship requirements for its cybersecurity major to mandatory, ensuring every student has the ability to complete this high impact practice and gain critical work experience in cybersecurity.
2. Work with local two-year colleges and four-year institutions to develop new academic degree and certificate programs in cybersecurity that are responsive to local employer needs.
    a. In the Cyber Prep program, Pikes Peak Community College developed a new academic degree in cybersecurity to supplement the existing cybersecurity certificate program embedded in the Computer Network Technology degree program. The college then sought four-year partners, signing articulation agreements with six colleges and universities willing to accept the degree as part of their four-year offerings. In addition, the college developed articulation agreements and concurrent enrollment plans with area high schools as part of the RAMPS pilot, allowing high school students to earn college credit and high school credit in their school's cybersecurity program.
    b. Old Dominion University (ODU) created an interdisciplinary major/minor in cybersecurity in Fall 2016 with courses drawn from multiple disciplines such as, philosophy, computer science, computer engineering, information technology, and criminal justice. This program has grown from 11 students to over 100 in just two years. Building upon the success of this program, ODU also developed two additional interdisciplinary majors: Cyber Operations and Cybercrime.

3. To boost enrollment and increase the cybersecurity workforce, the student body from community colleges should be developed and supported to allow easy transition into four-year cybersecurity programs.
    a. The University at Albany helped facilitate community college student entry into their university by developing 2+2 programs with articulation agreements so that the students can work through the entire four-year program starting at a community college. The 2+2 program has helped the students succeed, improving their performance. To get them ready for the four-year program, community college students are exposed to the same tools that the students at The University at Albany use such as virtual environments that can be accessed remotely.
    b. HRCyber worked with Old Dominion University and three community colleges (Northern Virginia Community College, Tidewater Community College, and Thomas Nelson Community College) to develop articulation agreements with the Associate of Applied Science in Information Technology Systems and the Bachelor of Science in Interdisciplinary Studies for Cybersecurity. These articulations agreements will save the transferring student over 50 credit hours, 1.5 years of time, and $16,500 in ODU tuition.
    c. Cin-Day Cyber provided three high school students who might have studied a field other than cybersecurity or computer science with a $5,000 college scholarship to further their education in cybersecurity and computer science. Scholarships are one of the best ways to grow the workforce pipeline that is experiencing a shortage, such as in the cybersecurity realm. Further, Cin-Day Cyber sponsored National Cybersecurity Career Awareness Week at area STEM middle and high schools.
    d. The Cyber Prep Program developed more technically-focused two-year programs at community colleges that can be linked to bachelor's degree programs at four-year schools. These programs can meet local talent needs for information technology professionals with deep cybersecurity knowledge and curriculum updates can be approved more quickly and graduates are work-ready sooner because community colleges are responsive to employer demand.
4. To provide hands-on training to students and reduce the gap between education and job readiness, cybersecurity labs should be built through industry and academia collaborations. Development costs can be shared across multiple stakeholders, allowing both students and organizational employees to benefit from training in the laboratories.
    a. The University at Albany built two cybersecurity and digital forensics teaching laboratories and two research laboratories in which they routinely worked with industry partners for both training and research.
    b. The University at Albany also worked with New York State Information Technology Services (NYSITS) to build a cyber range that will help train employees at NYSITS and students in the one-year Master of Science program focused on Cyber Operations.
    c. HRCyber assisted Old Dominion University with funding to expand its cybersecurity virtual lab and in opening it up to other educational institutions outside of the university network. This lab was able to provide a secure and user-

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

friendly environment for students and faculty to remotely engage in hands-on training.

d. Cin-Day Cyber assisted with the development of the Ohio Cyber Range, a statewide initiative. Further, Cin-Day Cyber worked with teachers in K-12 to earn certifications in teaching cybersecurity.

5. Build educational programs for executive professionals. It is impractical to assume that senior executives will gain a deep knowledge of cybersecurity during a short class or presentation; however, short and focused programs that provide enough understanding to be able to ask the right questions and make informed decisions are critical.
   a. The team at Pikes Peak Community College has developed specific modules for all members of the Colorado Springs-based National Cybersecurity Center to introduce them to basic cybersecurity concepts, practices, and issues. Designed for non-cybersecurity experts, the courses introduce state and local government managers to the importance of cybersecurity in their work.
   b. The University at Albany conducted professional training for executives and management during the New York State Cybersecurity Conference. The training provided guidance on how to make risk-based decisions for cybersecurity.

Activities for Learners

1. Create partnerships with the K-12 school districts across the region to engage students and their parents as early as possible in STEM programs, including cybersecurity. Start programs such as summer cybersecurity camps for middle and high school students which can be useful in creating a pipeline of students from high schools into college and university programs. Several points of caution are worth mentioning, such as these programs must be: 1) organized far in advance so that parents can plan summer activities for the family; and 2) very hands-on and entertaining to capture student imagination and interest. A poorly-run camp has the potential to turn students away from cybersecurity. The camp day should be split between education and other activities as students are not used to sitting for 6 to 8 hours each day studying the same topic. While developing hands-on activities can be time consuming, there are many cybersecurity camps being offered and sharing resources with other organizations can amortize development costs.
   a. An example of a K-12 program initiated by HRCyber includes “Cyber Saturdays” which provided both high school students and their parents with activities and information related to cybersecurity careers. A total of 92 students and 41 parents attended the two Cyber Saturday events. Another example is a K-12 school counselors’ workshop which brought together counselors, career coaches, and career and technical education (CTE) teachers to learn about education pathways leading to a career in cybersecurity and for them to share their best practices regarding cybersecurity courses and activities.
   b. The City of Virginia Beach hosts an annual STEM Trifecta where K-12 students and their teachers compete in three areas: Robotics Challenge, Cybersecurity Challenge, and a Maker Expo. Over 1,000 students from 71 schools participated in the June 2018 event. HRCyber promoted this event and encouraged its partners to participate as judges and mentors.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287

   c. To increase student interest, Cin-Day Cyber worked with middle and high school students on their CyberPatriot programs, holding camps and sponsoring teams that competed at local, state, and national levels. One of the area's schools won the state competition.
   d. The Cyber Prep program focused on engaging teens to consider careers in cybersecurity. Cyber Prep team members hosted Cyber Warrior Princess summer camps and weekend day events for over 50 middle school girls that incorporated learning technical skills, conducting hands-on computer work, and doing fun team building activities to engage and inspire them to explore cybersecurity.
2. Creating or engaging with student clubs are a great way of integrating different cybersecurity communities in the same institution.
   a. The University at Albany created three clubs: ISACA Student Club (student chapter), Cyber Defense Organization (cybersecurity competitions), and the Digital Forensics Association. These clubs have students from multiple academic department programs working together on events and activities, drawing programs closer by exposing students to different disciplinary approaches to cybersecurity. These clubs are also a great way to attract organizations to sponsor events, help students with interview skills and resumé reviews, and teach skill sets necessary for club activities such as hackathons and cybersecurity competitions.
   b. Old Dominion University started a Cyber Security Student Association in 2016 and in one year it grew to one of their largest student clubs. They sponsored several activities where speakers from local cybersecurity companies came in to share their experiences and discuss their career pathways. The Association also hosts an annual cybersecurity conference and capture the flag event.

Activities for Job Seekers

1. Start internship or cooperative education programs to create an early pipeline of students to industry, and build relationships between students and employers to improve retention of students locally. In addition, starting mentorship programs with local employers helps connect students with local businesses.
   a. HRCyber created a high school cybersecurity internship program where students spent 30 hours working as an intern for a local cybersecurity company. This initiative proved itself to be valuable experience for both the student and the employer. In one case, the company hired the high school student prior to graduation and another company continued the internships, using their own resources for three students over the summer.
   b. HRCyber also worked with the Virginia Space Grant Consortium to provide cybersecurity internships to students from across the state using the Commonwealth STEM Industry Internship program to place the interns. These internships were very successful and provided the students with valuable experience in cybersecurity. Twenty-six interns were placed during the RAMPS project and it continues with a total of 107 cybersecurity interns placed since January 2017.
   c. Cin-Day Cyber leveraged existing relationships with employers to add cybersecurity internships as a key strategy for meeting workforce demand.

Additionally, Cin-Day partnered with research universities to hold a Cyber Research Fair to bring industry together with students who presented their research findings.

d. Cyber Prep coalition members saw the need for a cybersecurity-specific Career and Technical Student Organization (CTSO) in middle and high schools for students to explore cybersecurity through competitions, and develop skills and leadership abilities as a way to supplement existing competitions like CyberPatriot. The result was the development of sudoCYBER, a student organization to support the adoption of a cybersecurity school curriculum that now has 19 chapters across Colorado.

2. Organize cybersecurity-specific job fairs to connect talent with industry. It takes great effort for employers to go to regular job fairs to screen out hundreds of job seekers and for job seekers to scan through a large number of employers. Cybersecurity-specific fairs will help narrow the search.
   a. The University at Albany started hosting annual Cyber Job Fairs, and several employers indicated that they preferred attending them over more general fairs because doing so provided a higher yield of qualified applicants. It is important to align the job fairs with the recruitment cycles of employers to ease the burden on the organizations that have a standard recruitment process.
   b. Cin-Day Cyber partnered with industry associations to host forums, workshops, and career fairs with guidance on identifying and recruiting job candidates, as well as building programs that increase student interest in the cybersecurity field. Additionally, Cin-Day Cyber held "Cyber Mixers" that brought industry partners together with cybersecurity department heads and career services directors so industry would have a better understanding of current higher education programs and the volume of students in the pipeline.

Outreach

1. Create an online presence to share progress and reports, including research on supply and demand, calendar of upcoming events, contact information for internship programs, and overarching information about cybersecurity initiatives.
   a. Cin-Day Cyber's website is an example that contains both rich content as well as visuals to display the accomplishments of the initiative.
   b. In collaboration with Pikes Peak Community College, the Colorado Springs Chamber of Commerce & Economic Development Corporation launched the website coloradospringscybersecurity.com. The site outlines resources for job seekers – including transitioning military – to pursue education, training, and employment. It also provides an asset map of local cybersecurity organizations, highlights resources to learn more about cybersecurity, and advertises events and activities.
2. Encourage participation in national gatherings of cybersecurity experts from education.
   a. Cin-Day Cyber funded 18 students to attend the 2017 NICE Conference which provided them a better understanding of cybersecurity career opportunities and allowed them to make industry connections.

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8287