The 3D Cybersecurity Pipeline: Bridging Schools, Higher Education, and Industry

Industry Survey Report 2025

Prepared by
Dr. Jennifer Penland
VSGC STEM Education Program Specialist
jpenland@odu.edu

Mr. Chris Carter
VSGC Director, Project PI
CXCarter@odu.edu

Executive Summary

Virginia is currently facing a significant cybersecurity workforce shortage, with only 75% of positions filled—below the national average. The state has over 50,000 cybersecurity job openings, including more than 11,000 requiring the CompTIA Security+ certification. In response, a coalition of educational institutions, industry partners, and community organizations launched the *3D Cybersecurity Pipeline: Bridging Schools, Higher Education, and Industry*. This grant-funded initiative is supported by the National Institute of Standards and Technology **(NIST),** the National Initiative for Cybersecurity Education **(NICE),** and the Regional Alliances and Multistakeholder Partnerships to Stimulate **(RAMPS)** Cybersecurity Education and Workforce Development.

Led by the Virginia Space Grant Consortium (VSGC), Virginia Peninsula Community College (VPCC), Brightpoint Community College (BCC), and Old Dominion University's Commonwealth Cyber Initiative – Coastal Virginia Node (COVE CCI), the project actively engages cybersecurity industry leaders across Virginia. Guided by feedback from 44 regional industry partners, this initiative is charting a bold course toward expanding access to cybersecurity education, enhancing skill diversity, and aligning workforce development with nationally recognized best practices. Industry collaboration remains the cornerstone of this effort—ensuring the creation of a scalable, inclusive talent pipeline that meets the dynamic demands of Virginia's cybersecurity sector.

Introduction

The central goal of this project is to build a cohesive network of cybersecurity stakeholders to strengthen the workforce pipeline in Virginia's eastern and central regions. The project team has fostered data-driven collaboration across public school systems, community colleges, four-year institutions, and industry partners through a *three-dimensional approach:* **Internships, Professional Development,** and **Industry engagement**. The Professional Development training was coordinated by Dr. Jennifer Penland (Grant Coordinator) and conducted in collaboration with Dr. Michael Mann (Professor at Virginia Peninsula Community College – Hampton campus) and Mr. Erik Breede (Phoebus High School). A post-training survey report will be developed to assess outcomes and inform future initiatives.

These regional alliances and multistakeholder partnerships are contributing to the development of the **Virginia Cybersecurity Pipeline: A Regional Blueprint for Education and Workforce Development**. The blueprint outlines academic course offerings, credentialing programs, certifications, and career opportunities, providing multiple entry points into the cybersecurity workforce pipeline tailored to each participating region. It also illustrates the various stages at which students engage with cybersecurity content and identifies clear, localized pathways to continue their education or enter the workforce. The blueprint serves as a strategic guide for educators, institutions, and employers to align efforts and resources, ensuring students are informed and supported throughout their journey into the cybersecurity field.

Second Dimension: Professional Development

The *Second Dimension* of the project focuses on strengthening the cybersecurity education pipeline from high school through postsecondary institutions and into the workforce. This phase has brought together educators, community colleges, universities, and industry partners to collaboratively design and implement a two-day professional development (PD) workshop aimed at building teacher capacity in cybersecurity instruction.

Educators who participated in the PD included high school teachers, dual enrollment instructors, and community college faculty from Brightpoint Community College and Virginia Peninsula Community College. The workshops featured immersive learning experiences aligned with the NICE Framework, emphasizing key cybersecurity workforce elements such as content knowledge, performance-based assessments, workplace skills, certifications, and career pathways.

During summer and fall 2025, the project team conducted surveys and training sessions to assess participants' cybersecurity content knowledge and familiarity with industry certification processes. These insights informed the development of targeted PD experiences that equipped educators to guide students toward meaningful engagement with cybersecurity and clearly defined pathways into the field.

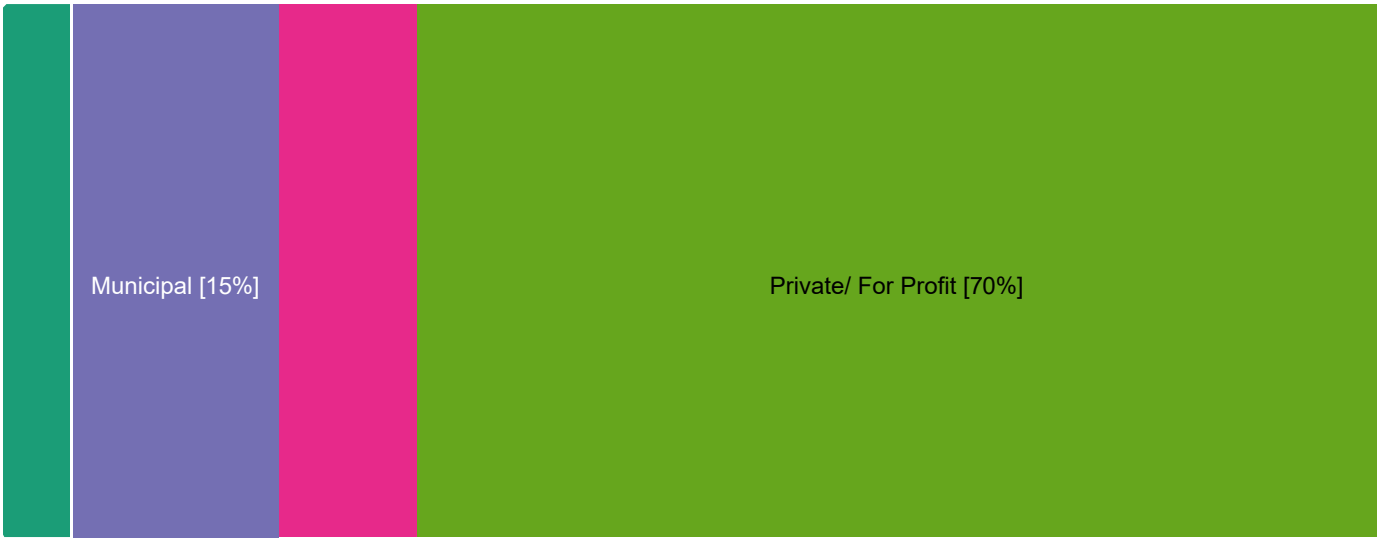
Planning, delivery, and classroom implementation support have been integrated throughout the project timeline to ensure sustained impact and alignment with workforce needs. Educator participants are preparing to present insights gained from the professional development training and propose changes to their existing courses during a **Fall 2025 Symposium**, with additional presentations scheduled for **Spring 2026**. These sessions will serve as platforms for sharing best practices, refining instructional strategies, and strengthening the connection between cybersecurity education and workforce readiness.

Workforce Survey Summary

The 2025 VSGC Cybersecurity Workforce Survey highlights ongoing gaps in both technical and soft skills across the cybersecurity labor market. Most respondents **(70%)** came from private and for-profit organizations, with half representing small businesses of 50 employees or fewer. Employers identified key technical competencies in high demand, including access controls, AI security, cloud security, and DevSecOps. Despite this, notable skill deficits persist—particularly in analytic capabilities **(29%),** technical proficiency **(20%),** and project management **(18%).** On the soft skills front, communication **(18%),** teamwork **(16%),** and emotional intelligence **(16%)** emerged as critical areas of need.

The **44 respondents** also emphasized the importance of enhancing curricula to better address threat intelligence, network security, and risk management, while integrating emerging domains such as AI, machine learning, and ransomware resilience. To close these gaps, the survey recommends expanding hands-on, real-world learning opportunities—such as internships, apprenticeships, and cooperative education programs—and strengthening partnerships between industry and academia to ensure curricula remain aligned with evolving threats. Ultimately, the findings underscore the need for a balanced approach that combines technical expertise, adaptability, and interpersonal effectiveness to prepare the next generation of cybersecurity professionals.

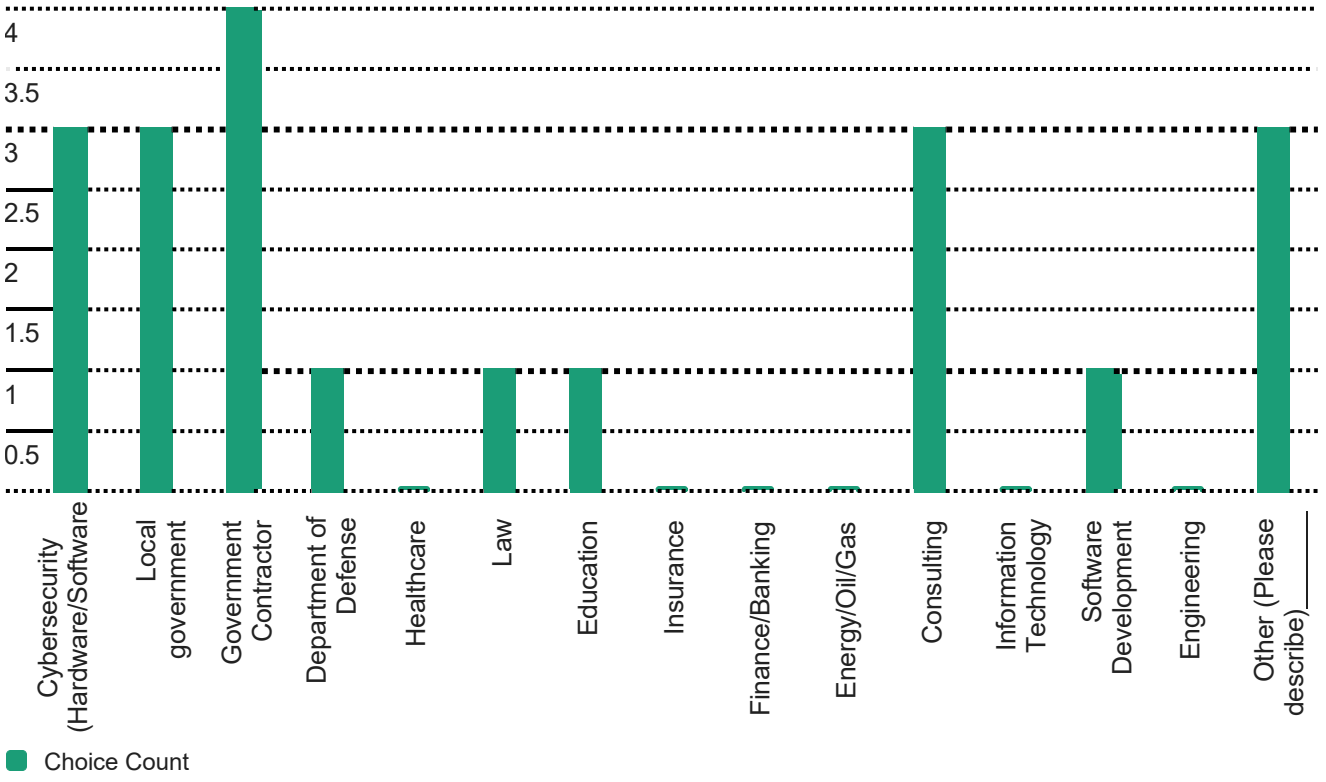
Q1 - Which of the following best describes your organization.



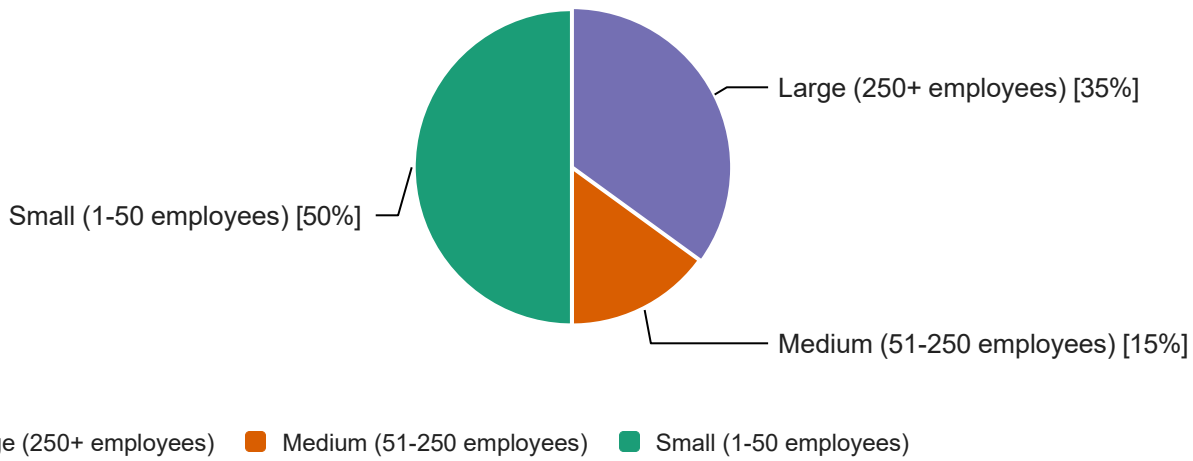
Federal [5%] State [0%] Municipal [15%] Not-for-profit [10%] Private/ For Profit [70%]

Other (Please describe)_____[0%]

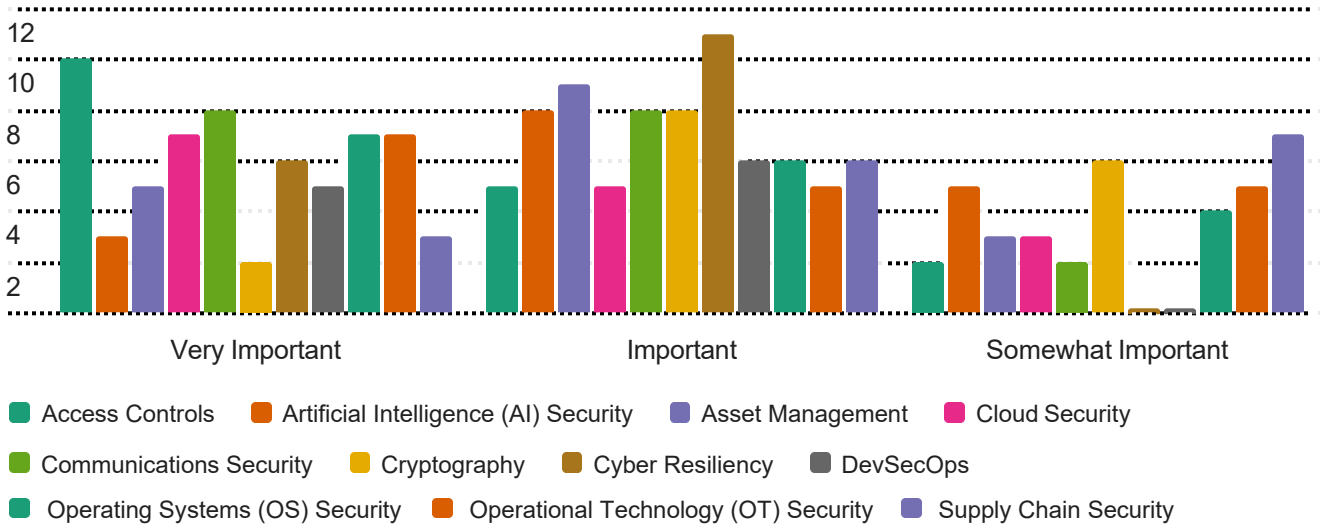
Q2 - Please indicate the main industry category that describes your company.



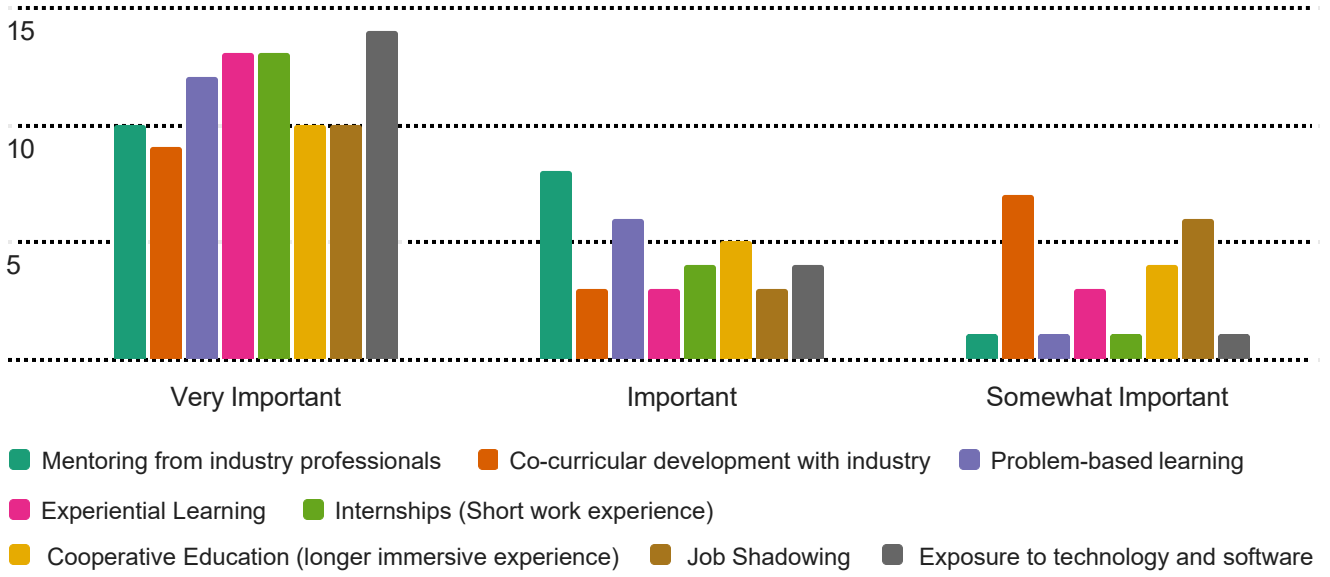
Q3 - How would you classify the size of your organization?



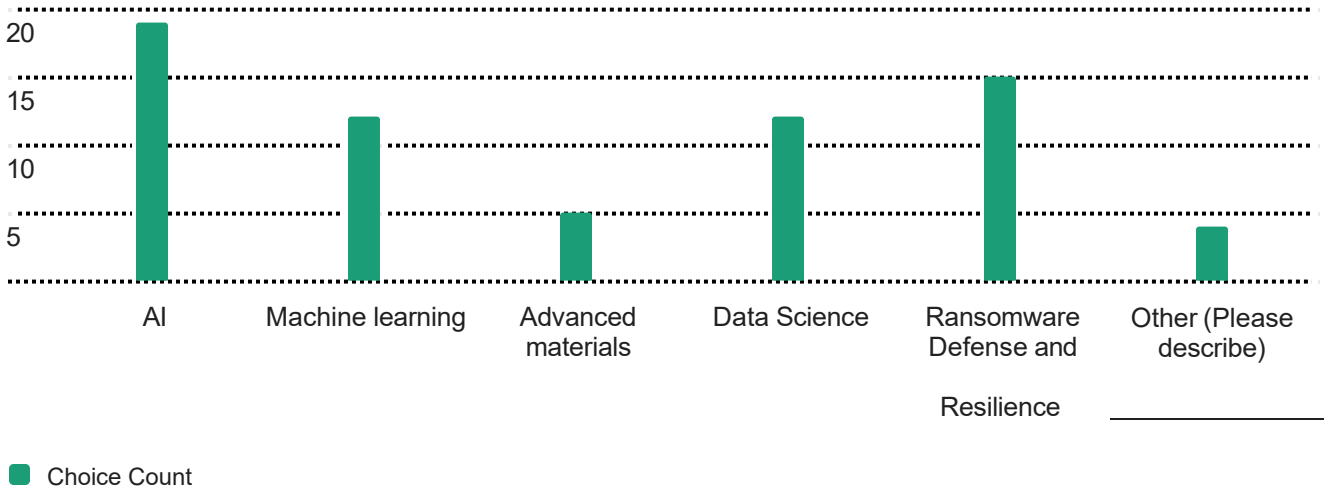
Q4 - Please rate how important knowledge and skills (Competencies) are when hiring.



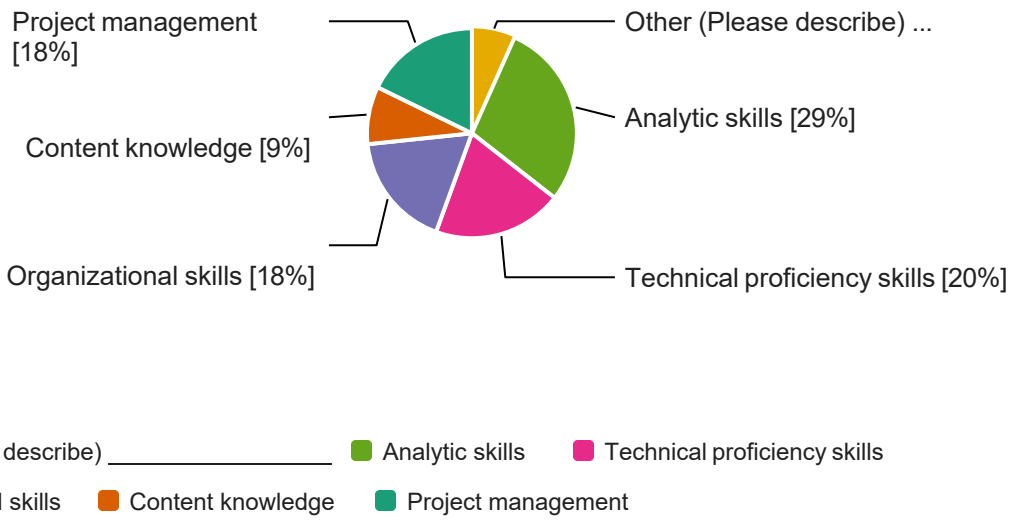
Q5 - Directions: Respond to the following on a scale from Very Important (4), Important (3), and Somewhat Important (2).



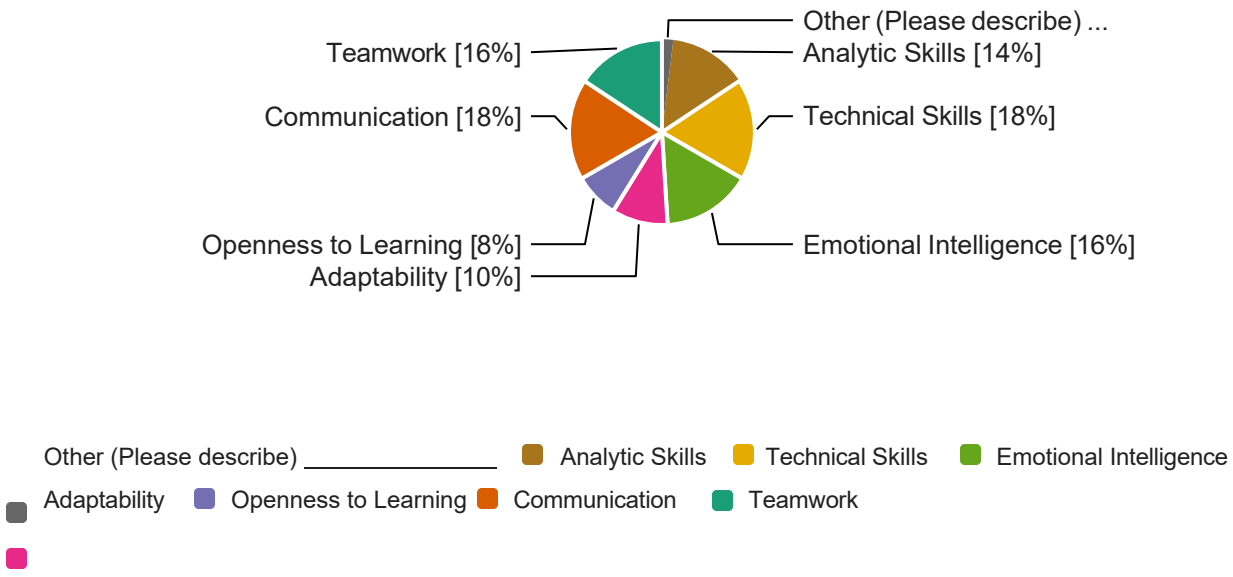
Q6 - Which emerging trends in your industry do you think should be incorporated into Cybersecurity education and training programs? (Click all that apply.)



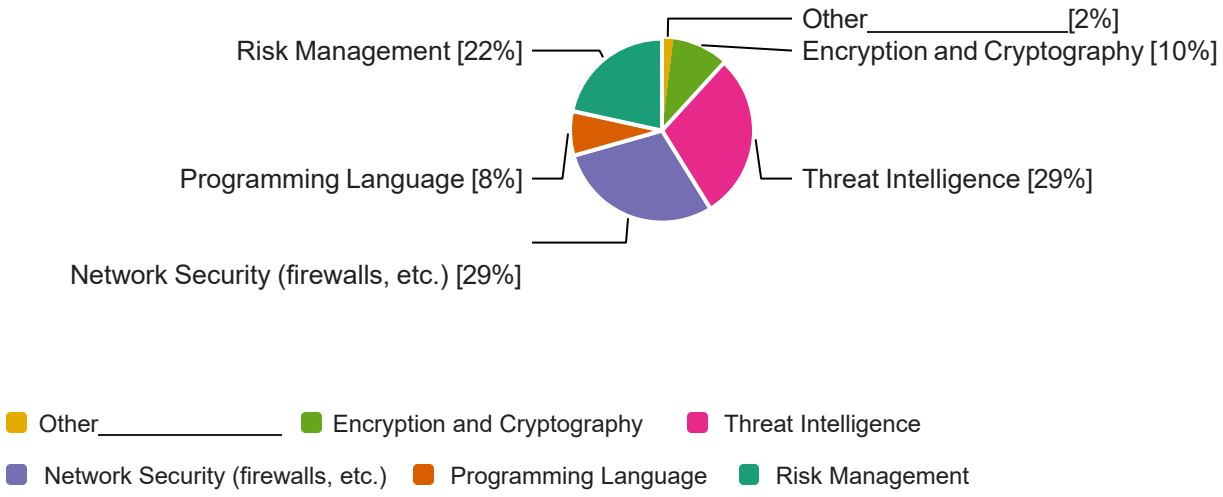
07 - What gaps, if any, do you see in the current professional (HARD) skill sets of recent graduates entering the Cybersecurity workforce? (Click all that apply.)



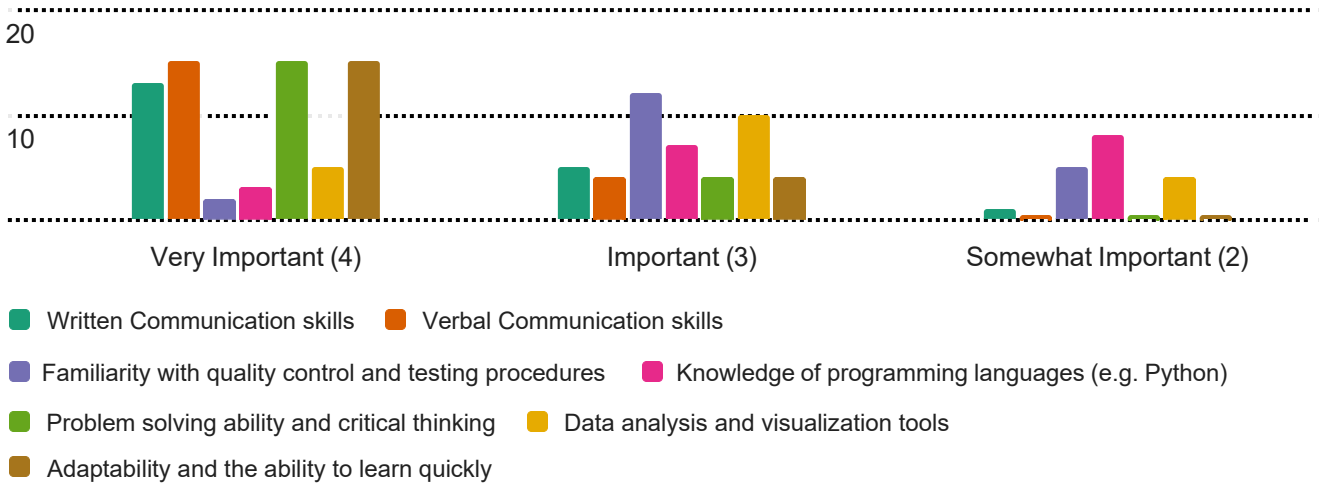
Q8 - What gaps, if any, do you see in the current professional (SOFT) skill sets of recent graduates entering the Cybersecurity workforce? (Click all that apply.)



Q9 - What specific skills or areas of knowledge would you like to see emphasized more in educational institutions (secondary and/ or higher education) curricula for future Cybersecurity industry professionals? (Click all that apply.)



10 - Directions: Respond to the following on a scale from Very Important (4), Important (3), and Somewhat Important (2).



Q11 - (Optional Response) What specific actions can educational institutions and workforce development programs take to better prepare the entry-level cybersecurity workforce?

hands-on, team-based work experiences. Continue the Space Grant consortium and its promotion of technology internships!

There are many very good practical videos on the web such as: 1) Having students build their own home labs, 2) practice using tools of the trade: Kali Linux, Splunk, 3) Using LLMs as assistants, tutors and mentors

Immerse students in real-world applications with seasoned mentors

Work on soft skills (communication, writing, etc.) vs hard skills (in lab experience)

Push hands on learning with public/private corporations to understand real world problems, continue learning problem solving and troubleshooting techniques.

Coding

Include digital twins in curricula...

Provide more hand-on labs to cover basic OS installation and configuration. Provide more hands-on labs covering typical cybersecurity tools, like vulnerability scanning and analysis.

Cybersecurity Apprenticeship programs so they can get clearances

Troubleshooting and critical thinking skills along with perseverance.

Theme Recommendations from Industry Respondents

- **Tailor curriculum to organization size:** Since medium-sized organizations are most represented, educational programs should align training with the needs of these employers, focusing on practical skills and scalable cybersecurity solutions.
- **Address hard skill gaps**: Institutions should enhance training in project management, technical proficiency, and analytic skills through hands-on labs, certifications, and real- world simulations.
- **Strengthen soft skills**: Communication, teamwork, and adaptability should be integrated into coursework via group projects, presentations, and interdisciplinary collaboration.
- **Industry collaboration**: Partner with cybersecurity firms and government agencies to co-develop curricula and offer mentoring, internships, and job shadowing opportunities.
- **Continuous feedback loop:** Establish regular surveys and advisory boards with
- industry stakeholders to keep educational content aligned with evolving workforce needs.
- **Emphasize emerging technologies**: Incorporate AI, machine learning, and
- ransomware defense into training programs to prepare students for future challenges.
- **Promote experiential learning**: Expand cooperative education and apprenticeship programs to give students immersive, real-world cybersecurity experience.

APPENDIX 1:
3D Cybersecurity Industry Survey

1. **Which of the following best describes your organization:**

    - Federal
    - State
    - Municipal government
    - Not-for-profit
    - Private/For-Profit
    - Other (please describe) _____

2. **Please indicate the main industry category that describes your company:**

    - Cybersecurity (Hardware/Software/Services)
    - Local government
    - Government Contractor
    - Department of Defense
    - Healthcare
    - Law
    - Education
    - Insurance
    - Finance/ Banking
    - Energy/Oil/Gas
    - Consulting
    - Information Technology
    - Software Development
    - Engineering
    - Other (please describe) _____

3. **How would you classify the size of your organization? (Common categories include:)**

    - Small (1-50 employees)
    - Medium (51-250 employees)
    - Large (25+ employees)

4. **Please rate how important the following knowledge and skills (Competencies) are when hiring for entry level positions with your organization Problem):**

NICE Competency Area	Very Important	Somewhat Important	Somewhat Unimportant	Not Important
Access Controls				
Artificial Intelligence (AI) Security				
Asset Management				
Cloud Security				
Communications Security				

Cryptography				
Cyber Resiliency				
DevSecOps				
Operating Systems (OS) Security				
Operational Technology (OT) Security				
Supply Chain Security				

Directions: Rank the following questions on a scale from most important to least important.

5. **Which of the following best prepares students for success in the Cybersecurity industry?**

    - Mentoring from industry professionals
    - Co-Curricula Development with Industry
    - Problem-based learning
    - Experiential Learning
    - Internships (short work experience)
    - Cooperative Education (longer immersive experience)
    - Job shadowing
    - Exposure to technology and software

6. **Which emerging trends in your industry do you think should be incorporated into Cybersecurity education and training programs?**

    - AI
    - Machine learning
    - Advanced materials
    - Data Science
    - Ransomware Defense and Resilience
    - Other _____

7. **What gaps, if any, do you see in the current professional (HARD) skill sets of recent graduates entering the Cybersecurity workforce?**

    - Project management
    - Content Knowledge
    - Organizational skills
    - Technical proficiency skills
    - Analytic Skills

8. **What gaps, if any, do you see in the current (SOFT) skill sets of recent graduates entering the Cybersecurity workforce?**

- Teamwork
- Communication
- Openness to learning
- Adaptability
- Emotional Intelligence
- Technical skills
- Analytic Skills

9. What specific skills or areas of knowledge would you like to see emphasized more in educational institutions (secondary and/or higher education) curricula for future Cybersecurity industry professionals?

- Risk management
- Programming Language
- Network security (firewalls, etc.)
- Threat Intelligence
- Encryption and Cryptography

Directions: Respond to the following questions on a scale from 4- Very Important, 3- Important, 2- Somewhat Important, 1-Not Important.

10. How important are:

- Communication skills (written) for entry-level positions in the Cybersecurity industry. [4 – Very Important; 3- Important; 2- Somewhat Important; 1-Not Important]
- Communication skills (verbal) for entry-level positions in the Cybersecurity industry. [4 – Very Important; 3- Important; 2- Somewhat Important; 1-Not Important]
- Familiarity with quality control and testing procedures in the Cybersecurity industry (e.g., NDT, stress testing, environmental simulations). [4 – Very Important; 3- Important; 2- Somewhat Important; 1-Not Important]
- Knowledge of programming languages such as C++, Python, or MATLAB for entry-level positions. [4 – Very Important; 3- Important; 2- Somewhat Important; 1-Not Important]
- Problem-solving ability and critical thinking. [4 – Very Important; 3- Important; 2- Somewhat Important; 1-Not Important]
- Data analysis and visualization tools (e.g., Excel, MATLAB, Python, R) for new hires. [4 – Very Important; 3- Important; 2- Somewhat Important; 1-Not Important]
- Adaptability and the ability to learn new technologies quickly in the fast-paced Cybersecurity industry. [4 – Very Important; 3- Important; 2- Somewhat Important; 1-Not Important]

---

11. What specific actions can educational institutions and workforce development programs take to better prepare the entry-level cybersecurity workforce?

The following individuals contributed to the development of the survey:
Rachel White, Ph.D., The Center for Educational Innovation and Opportunity, Old Dominion University. John Fife, Ph.D., Director of the Center for Innovation in STEM Education, Virginia Commonwealth University.