White Paper

Building and Enhancing U.S. Cybersecurity Education and Workforce Development Strategic Initiatives: Advancing National Infrastructure, Capability, & Capacity

ATARC Cybersecurity Education and Workforce Development Working Group

August 2024

ATARC

Advanced Technology Academic Research Center

Building and Enhancing U.S. Cybersecurity Education and Workforce Development Strategic Initiatives: Advancing National Infrastructure, Capability, & Capacity

Traditional and Non-Traditional Approaches to Cybersecurity Career Pipelines and Pathways

This Strategic Action Plan and Recommendations Report is prepared for the 118th (2023-2024) U.S. Congress and National Association of State Chief Information Security Officers (NASCIO)

Document Prepared by:
Dr. Keith Clement
Professor, California State University, Fresno
Academic Chair, ATARC Cybersecurity Education and Workforce Development Working Group

Advanced Technology Academic Research Center (ATARC)

ATARC Cybersecurity Education and Workforce Development Working Group

Executive Summary

Cybersecurity and digital critical infrastructure protection are critical national security and economic concerns in an era of significant geopolitical tension and conflict. Preventing, mitigating, reducing, and responding to these significant issues requires a prepared and skilled national cybersecurity workforce. However, cybersecurity workforce preparation capability and capacity has not kept up with explosive growth in the professional field. The rise of Artificial Intelligence (AI) has not helped the situation. Equilibrium between the numbers of cybersecurity professionals needed and the numbers prepared remains an elusive objective in a very dynamic security environment. Lots of risks to manage, vulnerabilities to sort out, and numerous threat/attack vectors to adapt quickly to. As cybersecurity continues to deepen its footprint within our societies and economies, we must be agile, swift, and innovative in national strategy to prepare national, state, and local cyber workforce development and career education through career pipeline and pathways.

There are many complex moving parts found within the cybersecurity domain and operational environment. One key driver of ecosystem capability gaps is a lack of skilled and experienced cybersecurity workforce in the existing labor pool. Cybersecurity education and workforce development is a complicated and salient problem for modern organizations, government institutions, the private sector, and our citizenry. The national issue of cybersecurity workforce development and education is of utmost importance given a well-known (and growing) global skilled workforce and skill gap. Securing cyber workforce development capability and education capacity is crucial for the evolution of the professional field, maturing academic discipline, and training providers. Cybersecurity education, training, and workforce development is key to vigilance in the complexity of cyberspace.

The meteoric rise of cybercrime and malicious actors is a strong motivation and justification to develop and implement cybersecurity workforce development and education strategy to enhance capability and capacity and reduce current (and future) workforce and skills gaps. The first objective of this recommendations report is to understand structural issues and additional factors driving current cybersecurity workforce capability and capacity gaps. Second, we present and describe a Framework for hardening campus information security & networks, campus critical infrastructure protection, and digital awareness programs. After all, education, teaching, and research need a safe and secure place for successful learning practices, processes, and collaboration found at the heart of American K-12 and Higher Education systems. Third, the report provides a series of recommendations to guide the formulation and promulgation of effective cybersecurity workforce development and education strategies as well as concrete steps to enhance the policies and “best practices” found within this critical sector. These three report objectives are organized into 9 paper sections to provide a comprehensive view of the cybersecurity professional preparation process and ways it can be enhanced and strengthened.

One key report feature is the discussion of a national cybersecurity career education pipeline and pathway that includes both a traditional "academic" and non-traditional "skills-competency" approach to professional preparation. The traditional pathway includes linked and aligned education programs from kindergarten through Ph.D. programs in cybersecurity (and adjacent areas like AI, Cyber Defense, Software Development, Programming, etc.) The non-traditional pathway relies on the Career Technical Education (CTE) approach, industry-based professional certifications, and workforce development models like registered apprenticeships, paid internship programs, co-ops, and On the Job Training (OJT) opportunities. Both approaches, or "pathways" are heavily steeped in the best practices of Diversity, Equity, Inclusivity, and Accessibility (DEIA) and supporting special populations in technology.

Key report findings and recommendations found in the following paper sections:

Cybersecurity workforce development and education has a variety of challenges, problems, obstacles, and structural limitations to overcome. A series of key recommendations are mapped out to structure a replicable cybersecurity education and workforce development pipeline and pathway strategy for utilization across the U.S. Based on these key cybersecurity workforce development and education capability and capacity issues, this report is organized into the following sections:

- Cybersecurity Workforce Development and Education (WDE) Challenges, Problems, Barriers, Obstacles, and Limitations (Section 1)
- A Framework for Hardening Campus Information Security & Networks; Campus Critical Infrastructure Protection & Digital Awareness Programs (Section 2)
- Cybersecurity K-12 Education (Section 3)
- The Traditional (Academic) Pathway Model- Cybersecurity Higher Education/Training Programs, Degrees, Certificates, Curriculum, and Standards (Section 4)
- The Non-Traditional (Experiential) Pathway Model- Building and Enhancing U.S. Cybersecurity Education and Workforce Development Infrastructure, Capabilities, & Capacity Through Professional Skills/Competency Development, Pre-Apprenticeships, Registered Apprenticeships, Internships, Cyber-competitions, Hackathons, and related (Section 5)
- Diversity, Equity, Inclusivity, and Accessibility (DEIA): Supporting Special Populations (Section 6)
- Cybersecurity Workforce Preparation- The Value of Industry Recognized Professional Certifications (Section 7)

- Cybersecurity Workforce Preparation: The Value of On the Job Training (Section 8)
- AI Risks and Opportunities (Section 9)

TABLE OF CONTENTS

EXECUTIVE SUMMARY 2
Key report findings and recommendations found in the following paper sections: 3
ABOUT ADVANCED TECHNOLOGY ACADEMIC RESEARCH CENTER (ATARC) .. 7
ATARC Cybersecurity Education and Workforce Development Working Group Information 7
ATARC Cybersecurity Education and Workforce Development Working Group Mission Statement. 7
ATARC Cybersecurity Education and Workforce Development Working Group Objectives 7
Acknowledgements 8
COMMONLY USED ABBREVIATIONS 10
KEY TERMS DEFINED 12
INTRODUCTION 14
STATEMENT OF THE PROBLEM 15
Cybercrime and Cybersecurity 15
Critical Infrastructure Protection and Resilience 16
The Meteoric Rise of the Cybersecurity Industry 17
Current Cybersecurity Workforce Capability Gaps 18
Current U.S. Cybersecurity Competency Skill Gaps 19
Strategic Action Plan & Recommendations Report Organization and Structure 19
Strategic Action Plan & Recommendations Report Objectives 20
SECTION #1 22
Cybersecurity Workforce Development and Education (WDE) Challenges, Problems, Barriers, Obstacles, and Limitations 22
Summary of Cybersecurity Workforce Development and Education Challenges 23
Cybersecurity Workforce Development and Education Challenges 23
Cybersecurity Key Stakeholders and Major Partner Challenges 24
Community-Based/ Neighborhood Organizational Challenges 26
Section 1 Conclusion 27
SECTION #2 28
Section 2 Overview 28
Part I - Strategies for Hardening Campus Information Security and Networks 34
Part II - Protecting Campus Critical Infrastructure 39
Part III - Enhancing Digital Awareness Programs 42
Summary of Section 2 Recommendations 46
SECTION #3 48
Cybersecurity K-12 Education 48
Section Introduction 48
Section Overview 48
K-6 Academic Support & Skill Development 49

Cybersecurity 7-12 Career Technical Education 49
STEM/STEAM 51
Cybersecurity Professional Development Events 51
Gamification: Cybersecurity Competitions, CTFs, and ESports 53
Digital Awareness and Information Literacy 53
K-12 Campus Infrastructure 55
K-12 Student Industry Recognized Professional Certifications 56
Dual Enrollment 56

K-12 EDUCATION RECOMMENDATIONS 57

SECTION #4 60

Section 4 Overview 60
Introduction 60
Section 4 Conclusion 72

SECTION #5 74

Section 5 Overview 74
The Value of Cybersecurity Non-Traditional Pathways 75
Section 5 Conclusion 76

SECTION #6 77

Section 6 Overview 77
Section 6 DEIA Recommendations 80
Section 6 Conclusion 82

SECTION #7 84

Section 7 Overview 84
Section 7 Certification/Credential Recommendations 88

SECTION #8 91

Cybersecurity Workforce Preparation—On the Job Training 91
Cybersecurity OJT Objectives 91
Effectiveness of On the Job Training 94
On the Job Training Models 95
Cybersecurity OJT Challenges 96
Cybersecurity On the Job Training Opportunities 98
Professional Development in Cybersecurity 101

SECTION #9 103

AI Risks and Opportunities 103
Background and Scope 103
AI Threats in Cybersecurity 103
AI Opportunities in Cybersecurity 104

CONCLUSION 105

About Advanced Technology Academic Research Center (ATARC)

ATARC Cybersecurity Education and Workforce Development Working Group Information

The Strategic Action Plan and Recommendations Report is a collaborative effort of a group of national and state cybersecurity workforce development and education Subject Matter Experts (SMEs) drawn from many professional backgrounds. The ATARC Cybersecurity Education and Workforce Development Working Group seeks the advancement and enhancement of national educational cybersecurity infrastructure and strategies for cybersecurity professional career education and preparation via an accessible career pipeline model composed of "traditional" and "non-traditional" pathways as described herein this report. The working group met for 18 months (2023-2024) to research, analyze, and prepare this report.

The objective of this report is to provide Cybersecurity Education, Workforce Development, and Information Security Officers/Personnel SMEs an opportunity to discuss key barriers in workforce preparation and securing campus infrastructure for both K-12 and Higher Education. An additional objective is the development and promulgation of comprehensive cybersecurity workforce development, education, and campus awareness recommendations for consideration by U.S. Congress and the National Association of Chief Information Security Officers. There are a variety of key perspectives to view this pressing problem from, including executive decision-makers, legislators, policymakers, government administration, as well industry sectors, employers of all sizes, school administrators, faculty, students, and Community Based Organizations (CBOs). This report is written for an audience well steeped in cybersecurity strategy and policy matters. This is a clear and present national and economic security issue.

ATARC Cybersecurity Education and Workforce Development Working Group Mission Statement

"Build a collaborative framework of key stakeholders to provide strategic recommendations on enhancing national cybersecurity education and workforce development policy and practice to implement an innovative and comprehensive national career pipeline/ pathway at all levels of education/training, accessible to everyone, and clearly communicated through detailed "road maps" for career preparedness and college readiness tracks." [1]

ATARC Cybersecurity Education and Workforce Development Working Group Objectives

1. Understand core obstacles, limitations, and challenges facing all key stakeholders and major partners in cybersecurity workforce development and education.

[1] https://atarc.org/cyber-higher-education/ Accessed electronically on 2/14/2024.

2. Develop and maintain working group collaboration and partnerships to complete a number of activities, initiatives, deliverables, and pilot projects in progress. It is critical that industry (employers), academia, the public sector, and community/ neighborhood-based organizations work together collaborating and craft viable solutions.
3. Enhance and support national and state-level cybersecurity education, workforce development, and initiatives through pilot program design, implementation, and evaluation.
4. Analyze and evaluate cybersecurity workforce development and education policies, best practices, and common ways of professional preparation into quickly evolving "high demand and hard to fill" positions currently found within the cybersecurity field.
5. Align, link, and coordinate cybersecurity education, training, and workforce development practices into a seamless, easy to transition career education pipeline and pathway spanning K-12 Education and Higher Education to include both a "traditional approach" (academic) and "non-traditional approach" (skills-competency based).

Acknowledgements

This Strategic Action Plan and Recommendations Report was a collaborative writing project amongst many participants and contributors. These cybersecurity workforce development and education recommendations are the result of the dedication and efforts of many Subject Matter Experts (SMEs). We met monthly for 18 months and reviewed many paper drafts as a group. We want to acknowledge and thank everyone for their contributions, work, and efforts in the completion of this report. Sincere apologies for those who may have contributed to the paper, but were left off the acknowledgements list inadvertently.

Eric Wall, Chief Information Security Officer, University of Arkansas System

Gregory W. Cooper, Information Systems Operations Center (ISOC) Manager, New Mexico State University Physical Science Laboratory

Patrick Slattery, Director of Industry Engagement, Zicklin School, Baruch College, City University of New York (CUNY)

Dr. Chuck Gardner, Senior Advisor for Workforce Development, Cyber Innovation Center

Emily Harris, CISSP, Higher Education Cybersecurity Professional

Dr. Abdallah Haddad, Chief Information and Technology Officer, Lander University, SC

Jeff Angle, Senior Director, Academic and Workforce Development, ISACA

Dr. Ulku Clark, Director of Center for Cyber Defense Education, University of North Carolina, Wilmington

Joe Gibson, Information Security Officer, Trident Technical College, SC

Michael P. Melore, CISSP, Public Sector Security Ambassador and Senior Cyber Security Advisor, IBM Security

Mike Nicholson, ATARC Cybersecurity Advisor Chair

Troy L Adams, US Department of Health & Human Services, Northern Arizona University

Richard Braden, Managing Director of CompTIA Apprenticeship for Tech

Wesley Alvarez, Director of Academics, EC-Council

Sarah Carlson, Academic Development Manager, EC-Council

Bilge Karabacak, Assistant Professor of Cybersecurity, University of North Carolina Wilmington and Adjunct Professor, Franklin University

Ashwini Jarral, Director IJIS Institute (501(c)3 Non-Profit

Christine Whalley, CISO, Amherst College

Dr. Mohsen Beheshti, Professor, California State University, Dominguez Hills

Dr. Assefaw Gebremedhin, Associate Professor, Washington State University

Mark Odom, Vice President CTO & CISO, Thomas Jefferson University, Jefferson Health; Jefferson Health Plans

Kere Harper, Account Executive, Pluralsight

Commonly Used Abbreviations

(AI)	Artificial Intelligence
(ATARC)	Advanced Technology Academic Research Center
(CTF)	Capture the Flag
(CTE)	Career Technical Education
(CAE-C)	Center Of Academic Excellence in Cybersecurity
(CBO)	Community Based Organization
(CO-OP)	Co-Operative
(CMMC)	Cybersecurity Maturity Model Certification
(CISA)	Cybersecurity Information Security Agency
(CISM®)	Certified Information Security Management
(DHS)	Department of Homeland Security
(DEI)	Diversity, Equity, Inclusivity
(DEIA)	Diversity, Equity, Inclusivity, Accessibility
(ELT)	Experiential Learning Theory
(FERPA)	Federal Education Records Protection Act
(GLBA)	Gramm-Leach-Billey Act
(HIMSS®)	Healthcare and Information and Management Systems Society
(HIPAA)	Health Insurance Portability and Accountability Act
(HR)	Human Relations
(ICU)	Intensive Care Unit
(IT)	Information Technology
(IoT)	Internet of Things
(ISACA)	Information Systems Audit and Control Association
(LLM)	Large Language Model

(MET)	Manufacturing Engineering Technology
(ML)	Machine Learning
(MNC)	Multi National Corporation
(NASCIO)	National Association of State Chief Information Officers
(NICE)	National Initiative Cybersecurity Education
(NIST)	National Institute of Standards and Technology
(NSA)	National Security Agency
(NGOs)	Non-Government Organizations
(NSAs)	Non State Actors
(OJT)	On-the-Job Training
(Ph.D.)	Doctor of Philosophy
(PCI-DSS)	Payment Card Industry Data Security Standard
(PDS)	Primary Driving Standard
(SOX)	Sarbanes-Oxley Act
(STEM)	Science, Technology, Engineering, and Math
(STEAM)	Science, Technology, Engineering, Arts, and Math
(SME)	Subject Matter Expert
(SWOT)	Analysis Strengths, Weaknesses, Opportunities, and Threats
(USDOL)	United States Department of Labor
(USD)	United States Dollar
(WDE)	Workforce Development and Education
(WEF)	World Economic Forum

Key Terms Defined

Key Term	Meaning
Advanced Persistent Threat (APT)	A prolonged, targeted cyberattack where an intruder remains undetected to steal data, or a criminal organization with that intent.
Backdoor	A method for establishing and utilizing unauthorized access to a computer system, often installed by malware.
Botnet	A network of infected private computers (sometimes as simple as webcams or smart devices) controlled as a group for malicious tasks.
Business Continuity and Disaster Recovery	Plans to ensure critical functions continue during and after a disruption, where Business Continuity employs interim measures to continue operations and Disaster Recovery returns normal processing.
Critical Infrastructure Protection (CIP)	Safeguarding essential systems and assets vital to national and economic security. In the US, CISA and the Federal Government define and support activities in areas determined critical infrastructure.
Cybercrime	Criminal activities involving computers and networks, such as hacking and data breaches, though the means employed may be nontechnical.
Cybersecurity Competitions	Events challenging participants with various cybersecurity skills to develop practical experience competing in a simulation environment.
Cybersecurity Workforce Development	Efforts to build and enhance skills for individuals entering the cybersecurity field and the advance the skills required of those in the field. The required skills grow as cybercrime techniques advance.
Data Encryption	Converting data into a coded format to prevent unauthorized access.
Denial-of-Service (DoS) Attack	An attack to shut down a network or web resource (e.g. website) by overwhelming it with traffic.
Digital Awareness Programs	Initiatives to increase understanding of cybersecurity threats and safe online practices in business and personal environments.
Distributed Denial-of-Service Attack	A DoS attack using multiple systems to overwhelm a single target. May employ a botnet for scale.
Diversity, Equity, Inclusivity, and Accessibility (DEIA)	Ensuring fair treatment and opportunities for all individuals in cybersecurity. Continuous attention to the contributions a diverse community of individuals can contribute to cybersecurity.
Endpoint Security	Securing end-user devices from exploitation by malicious actors.
Ethical Hacking	Legally breaking into systems to identify and help fix security vulnerabilities in accordance with the systems owner(s) agreement.
Exploit	Software or data used to take advantage of a vulnerability in a system.

Key Term	Meaning
Firewall	A network security device that monitors and controls incoming and outgoing traffic based on security rules or algorithms.
Information Sharing and Analysis Center (ISAC)	A dedicated center that ingests and shares threat intelligence to its members, often within an industry sector, critical infrastructure area, or other cohort of like organizations.
Intrusion Detection Systems (IDS)	Devices that monitor network traffic for indicators of unauthorized access. These systems are often the first line of cybersecurity defense.
Malware	Malicious software designed to cause damage to a network, computer, or other digital device/asset.
Multi-Factor Authentication (MFA)	A security system requiring multiple forms of identification to verify a user. Often characterized as requiring a mix of means including *something you know*, *something you have*, *or something you are*.
Network Segmentation	Dividing a network into smaller segments to improve security and manageability. Segmentation aids intrusion detection and analysis.
Neurodiversity	Recognizing and valuing the unique strengths of individuals with neurological differences for the valuable skills they offer.
Patch Management	Regularly deploying updates to keep software secure from vulnerabilities. Applies to both applications and operating systems.
Penetration Testing (Pen Testing)	Evaluating the security of a system by simulating attacks to identify vulnerabilities. Often conducted in a predefined scope.
Phishing	Attempting to gather personal information through deceptive emails and websites. AI and other techniques are often employed.
Ransomware	Malicious software that blocks access to a system until a ransom is paid. System recovery does not guarantee there will not be recurrence.
Security Information and Event Management (SIEM)	Tools providing a holistic view of an organization's information security landscape through aggregation of inputs from various security tools (IDS, etc.)
Security Operations Center (SOC)	A centralized unit that handles security issues on an organizational and technical level. Large organizations may employe regional SOCs.
Social Engineering	Manipulating individuals to divulge confidential information.
Threat Intelligence	Information about threats and threat actors to help mitigate potential attacks. ISACs may share such information with sectors.
Two-Factor Authentication (2FA)	A security process requiring two forms of identification for access. The first level of Multi-Factor Authentication (defined above).
Vulnerability Assessment	Identifying and prioritizing vulnerabilities in systems, applications, and networks. Vulnerabilities expose assets to threats, creating risk.
Zero Trust Architecture	A security model requiring continuous verification of users for access to data and applications. Additional later beyond firewall protection.

Introduction

American society, like many others, relies heavily on Information Technology (IT), Computing, the Internet, and the billions of devices connected to the Internet of Things (IoT). The safe utilization of tech is heavily dependent on an ability to secure, protect, and defend data, computers, networks, privacy in all things digital and electronic. This objective has become even more challenging in recent years given significant geo-political conflict, the accelerating pace of innovative emerging technologies, and the increasing role of computing and data in a digital era. This rise of machines and applications has been as meteoric as the role of cybersecurity in our organizational and individual lives. Because of a quickened pace of technological innovation and the speed of the digital ecosystem, U.S. cybersecurity workforce development, education and related infrastructure has been put to the test. Unfortunately, this situation is not news to anyone, including strategic adversary states, Non-State Actors (NSAs), organized hacker collectives, and criminal ransomware gangs. Cybersecurity and vulnerability will remain a daunting national and economic security challenge until feasible strategies and effective solutions are designed and implemented.

Agility, nimbleness, and often technical skills are essential to success in the cybersecurity and information security domain. Enhanced and sophisticated cybersecurity capabilities rely on a trained and skilled cybersecurity workforce to keep America operating and innovating into the future. However, national cyber capabilities are limited by difficulty in talent acquisition and job retention given a byzantine maze of workforce development, education, training, and awareness barriers, obstacles, and limitations. As such, significant national and state cybersecurity domain workforce capability and skills gaps exist across all phases of the cybersecurity professional preparation process from entry-level through advanced work roles. Common industry talent acquisition models struggle to fill introductory positions, but also with retention of management and senior positions and highly specialized work roles as well (e.g. all the way up the career ladder).

Persistent cybersecurity workforce, education, and capability-skills gaps plague the private and public sectors as well as critical industry economic sectors. Given current geopolitical instability, the rise of near-peer non-democratic strategic adversaries, and the fundamental role of cybersecurity within our societal, organizational, and individual lives; we must find an accessible, effective, and comprehensive approach to preparing the tremendous amount of cybersecurity professionals necessary to meet existing critical needs. These issues are further murkier and amplified with new and emerging technologies like Artificial Intelligence (AI) and Machine Learning (ML) further roiling and generating change in the tech ecosystem.

The purpose of this recommendations report is to analyze and evaluate critical issues in national Cybersecurity Workforce Development & Education strategy and policy. As a group of Subject Matter Experts in this policy area, we develop and promulgate key recommendations to remedy and mitigate current critical cybersecurity WDE capability and capacity issues. Long-term

sustainable solutions are essential to meet national cybersecurity workforce gaps and manage risk, reduce vulnerability, and respond to threats to U.S. critical infrastructure.

Statement of the Problem

Cybercrime and Cybersecurity

There are many pressing issues in cybersecurity. Cybercrime impacts the global and national economy. Recent reports from the World Economic Forum (WEF) indicate that cybersecurity is the third largest economy in the world after the U.S. and China. [2] Cybersecurity Ventures anticipates world-wide cybercrime costs to increase annually from $3 trillion (USD) in 2015 to $10.5 trillion (USD) by 2025– or 15% increase yearly. [3] "According to Cybersecurity Ventures, the global annual cost of cybercrime is predicted to reach $9.5 trillion USD in 2024. Compounding this is the rising cost of damages resulting from cybercrime, which is expected to reach $10.5 trillion by 2025." [4] Comparitech estimated 88.5 million global cybercrimes globally annually with an average victim loss of $8,069 per crime, resulting in an annual estimated loss of $714 billion for victims. [5] This is a lot of cybercrimes and victims left in the aftermath.

Cybercrime can be very lucrative for state actors as well as non-state actors with the necessary skills. As such, we see malicious actors engaging in fraud, theft, and numerous additional problems for law enforcement and the broader criminal justice system. Cybercrimes and digital victimization occur through a variety of threat vectors and often utilize innovative exploits and attack methods. Additional factors like significant growth of IoT complicate the cybersecurity environment. For example, there are over 15 billion connected IoT devices globally (2023) and expected to double to 30 billion by 2030. [6]

There are numerous malicious actors (both state-level and non-state-level actors) organized and regularly launching attacks, running botnets, engaging in industrial espionage, or threatening critical industry sectors. Ransomware gangs are frequently a step or two ahead of prospective victims, law enforcement, organizational and corporate security teams, criminal

---

[2] https://cybernews.com/editorial/cybercrime-world-third-economy/ Accessed electronically on 1/27/2024.
[3] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ Accessed electronically on 1/27/2024.
[4] https://www.esentire.com/resources/library/2023-official-cybercrime-report Accessed electronically on 1/27/2024.
[5] https://www.comparitech.com/blog/vpn-privacy/cybercrime-cost/#Key_findings Accessed electronically on 1/25/2024.
[6] https://explodingtopics.com/blog/number-of-iot-devices Accessed electronically on 1/27/2024.

justice, intelligence agencies, and legislative bodies. It is challenging to keep up with cybercrimes and cyberattacks through legislation and policies intended to combat these dynamic information security problems today.

International cybercrime and cybersecurity issues have languished with a lack of information sharing and collaboration given the current global security and armed conflicts worldwide. Increased digital threat environment trends in ransomware and malware suggest that cybercrime (and the illicit funds generated) are not going anywhere anytime soon. If not kept in check, we will see an increase in these alarming trends, especially as AI technology converges and further impacts an already dynamic cybersecurity space (e.g. please see the report Section 9 discussion).

Critical Infrastructure Protection and Resilience

Ensuring the protection and resilience of critical infrastructure is a matter of national security. These systems form the backbone of essential operations and services that support our daily lives and the functioning of a modern society. In an increasingly interconnected and digitized world, cybercrime poses a significant risk and increases the need for a robust and prepared cybersecurity workforce. Cyberattacks on critical infrastructure sectors, such as energy, transportation, healthcare, and financial services, can have far-reaching and devastating consequences including disruptions to essential services, economic losses, threats to public safety, and national security. For more information on the sixteen sectors of critical infrastructure and what CISA is doing to support critical infrastructure security, please follow this link: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience.

The ever-evolving nature of cyber threats, coupled with the complexity of critical infrastructure systems, necessitates a highly skilled and adaptable cybersecurity workforce capable of effectively detecting, mitigating, and responding to these threats. A strong national emphasis on critical infrastructure protection and resilience must go hand in hand with concerted efforts to develop and maintain a talented cybersecurity workforce. This includes investing in cybersecurity education and training programs, fostering public-private partnerships, and promoting ongoing professional development opportunities. By cultivating a highly skilled and knowledgeable cybersecurity workforce, the nation can better safeguard our collective security and critical infrastructure, enhance resilience to potential disruptions, and maintain the continuity of essential services vital to the well-being of our citizenry, government, and economy.

Protecting critical infrastructure from cybercrime and cyberattacks is a significant national priority that necessitates a robust cybersecurity workforce. As critical systems and services become increasingly digitized and interconnected, they become more vulnerable to cyberattacks intended to disrupt essential operations, inflict economic damage, and compromise public safety. The complex nature of these systems and the constantly evolving cyber threat landscape demands a highly skilled and capable cybersecurity workforce.

Consequently, efforts to enhance critical infrastructure protection and resilience must be coupled with strategic initiatives to develop and maintain a talented cybersecurity workforce through education, training, public-private collaboration, and professional development opportunities to better secure vital national assets against crippling cyberattacks. A lacking strategic cybersecurity WDE action plan and comprehensive policy activity poses a significant national and economic security risk for today and tomorrow. This is particularly troubling given the recent rise of the cybersecurity industry and resulting employer demand for cyber talent acquisition and retention.

The Meteoric Rise of the Cybersecurity Industry

There is no shortage of news coverage of cyber-attacks and breaches, and reports of consumer data and passwords floating around the dark net. Probing attacks of federal, state, and local critical infrastructure and networks seems commonplace today. Given significant economic, legal, political, and privacy concerns arising in the current cybersecurity ecosystem, we are watching a meteoric rise of the cybersecurity industry, These proactive and reactive policies and administrative controls deal with cybercrime, critical infrastructure protection, and resiliency.

Cybercrime is a growing industry. [7] "The global indicator 'Estimated Cost of Cybercrime' in the cybersecurity market was forecast to continuously increase between 2023 and 2028 by a total $5.7 trillion U.S. dollars (+69.94 percent). After the eleventh consecutive increasing year, the indicator is estimated to reach $13.82 trillion USD and therefore a new peak in 2028." [8] Because of the increase in cybercrime and cyberattacks on critical infrastructure, we are watching the evolution, continued growth, and robustness of the cybersecurity industry. Cybersecurity insurance is an example of a new industry segmentation found in the growing professional service sector under the broader umbrella of IT and Security.

A meteoric rise, growth, and expansion in cybersecurity and adjacent fields is driving strong demand for a prepared, skilled, and experienced professional workforce. While the cybersecurity industry continues substantial growth and evolution, effective talent acquisition and retention strategies struggle to keep up with industry/ employer demand. This is due in part to the difficulty of finding a sufficient labor pool of prepared and experienced employees to fill out information security offices and teams. The cybersecurity workforce development and education issue will persist until adequate steps are taken to increase the number of qualified and skilled cybersecurity career professionals, including those drawn from traditionally underrepresented groups in tech and cybersecurity.

---

[7] https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide Accessed electronically on 1/25/2024.

[8] https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide Accessed electronically on 1/25/2024.

These current cybersecurity job openings and competency/skill gaps are briefly highlighted in the following report section to draw attention to the magnitude and scale of these gaps. There are two fundamental points to consider here—the number of available cybersecurity positions and the skill-competency levels of those found in these positions. Both points will be discussed in further detail next.

Current Cybersecurity Workforce Capability Gaps

A meteoric rise in cybersecurity across the world has fueled significant professional, management and workforce demand. There are many cybersecurity jobs currently available at the global, national and state level. The size of the global cybersecurity workforce was estimated at 5.5 million—a 9% increase from 2022. [9] The international cybersecurity workforce gap is estimated at 4 million available positions. [10] As the gap increases between numbers of cybersecurity jobs available and the supply of prepared workers for these positions, substantial workforce capability gaps will persist.

According to CyberSeek data, there are a total of 1,239,018 total employed cybersecurity workforce and a total of 469,930 current total cybersecurity job openings in July 2024. 11 The national cybersecurity workforce supply/demand ratio is 85% (i.e. there are only enough cybersecurity workers in the U.S. to fill 85% of the cybersecurity jobs that employers demand). 12

CyberSeek job openings are further broken down to state-level cybersecurity job openings and found below in Table 1. Nine states together account for 53.2% of current available national cybersecurity jobs. Many cybersecurity jobs are clustered in a relatively few American states. Cybersecurity workforce and job demand in these states would be a good place to start for an operational cybersecurity career education pipeline/pathway framework.

Table 1: 2024 U.S. States with Most Cybersecurity Job Openings

State	Cybersecurity Job Openings	% U.S. total Cyber Positions
U.S.	469,930	
Virginia	53,520	11.4%
California	39,616	8.5%
Texas	36,908	7.9%

[9] *ISC2 Cybersecurity Workforce Study,* 2023.
[10] https://blogs.worldbank.org/en/digital-development/hacking-cybersecurity-skills-gap-developing-countries Accessed electronically on 1/25/2024.
[11] CyberSeek https://www.cyberseek.org/heatmap.html Accessed electronically on 7/1/2024.
[12] CyberSeek https://www.cyberseek.org/heatmap.html Accessed electronically on 7/1/2024.

Maryland	27,730	6.0%
Florida	23,424	5.0%
Illinois	20,040	4.3%
New York	17,143	3.6%
Georgia	15,007	3.2%
Colorado	15,280	3.3%
Totals		53.2%

Source: CyberSeek https://www.cyberseek.org/heatmap.html Accessed electronically on 7/1/2024.

Current U.S. Cybersecurity Competency Skill Gaps

In addition to significant numbers of currently unfilled cybersecurity jobs, there is another concern related to existing workforce skills capability gaps as well. A cybersecurity "skill gap" is the disparity in demand for skilled cybersecurity professionals and the available workforce in terms of their relevant cybersecurity knowledge, skills, and abilities. 13 Industry surveys/statistics found significant cyber industry concerns. For example, 92% of cybersecurity professionals say their organizations suffer from skill gaps in one or more areas. 14 These skill gaps are often viewed internally as worse than the employee shortages themselves (59%). 44% of respondents indicated that their organizations can't find people to hire with the skills we need. 15 For the record, such issues often impact both entry level personnel and more advanced roles as well. Competency based skill gaps often range up the career ladder and should not be viewed as only an "intro job" problem. This problem exists for longer-term employees and impacts retention and performance as well.

In a nutshell, both cybersecurity workforce capacity issues and competency skill gaps are significant issues to resolve and strengthen for national and economic security, critical infrastructure protection, and societal resilience. The organization and structure of the Strategic Action Plan and Recommendations Report is discussed in the following section.

Strategic Action Plan & Recommendations Report Organization and Structure

Throughout the cybersecurity professional preparation process, there are several factors that contribute to a workforce bottleneck. The cybersecurity workforce development and education

---

[13] Brij Gupta, https://medium.com/@gupta.brij/navigating-the-cybersecurity-skill-gap-strategies-for-building-a-resilient-workforce-394866b6faa4# Accessed electronically on 6/30/2024.
[14] *ISC2 Cybersecurity Workforce Study*, 2023.
[15] *ISC2 Cybersecurity Workforce Study*, 2023.

ecosystem is complex, dynamic, and advances quickly. This is a nexus policy area comprised of emerging technologies (like AI and cybersecurity) K-12 Education, Higher Education, the workforce development/training community, the public and private sectors, CBOs, and additional key partners and major stakeholders. The cybersecurity preparation process encompasses a variety of academics, degrees, industry-based certifications, work experience, and professional development/networking skills. The totality of the preparation process includes Strengths, Weaknesses, Opportunities, and Threats (SWOT).

High demand-hard to fill positions often utilize cutting edge "in-demand" skill sets and competencies in cybersecurity and emerging technologies like AI. Tech and security job titles, position descriptions, work roles, and KSAs change over time given the innovative nature of the tech field. Thus, the cybersecurity professional preparation process, curriculum, best practices, uses cases, etc. must adapt and change regularly as well.

One key reason for the cybersecurity workforce development and education problem is the steep learning curve found in the cybersecurity professional preparation and hiring processes. The cybersecurity professional preparation process is rigorous with four important cybersecurity workforce preparation components (i.e. to meet typical minimum and preferred position requirements).

These preparation components include:

1. K-12 and Higher Education/Workforce Training- (Degrees/Certificates, etc.)- (Sections 3,4,5,6)
2. Professional industry-based certifications (Section 7)
3. Work experience/ On the Job Training (Sections 5, 6, 8)
4. Professional Development and Networking (Sections 5, 6,8)

ISC2 estimates the profession needs to almost double to be at full capacity. [16] As the gap between number of jobs available and prepared job candidates increases, we need to significantly expand cybersecurity infrastructure, capacity, and capability through the operation of an efficient cybersecurity career education preparation pipeline and pathway. An efficient solution to achieve this goal is one key report theme. Specific report objectives are found below.

Strategic Action Plan & Recommendations Report Objectives

Cybersecurity Workforce Development and Education Strategic Action Plan and Recommendations Report objectives include the following.

1. Understand the current barriers, obstacles, and limitations in cybersecurity education, training, and workforce development. (Section 1)

[16] *ISC2 Cybersecurity Workforce Study,* 2023.

2. Provide meaningful recommendations to the higher education community and major stakeholders and key partners to significantly increase a prepared and qualified cybersecurity workforce and reduce existing capability and skill gaps found nationally. (Sections 2-9)
3. Enhance national cybersecurity readiness, preparedness, and response capability, and capacity; boost our national and state preparedness.
4. Develop a seamless, comprehensive cybersecurity education program across all levels of education (K-12 and Higher Education); including alignment, linkages, and transitions.
5. Develop mechanisms to link and align professional industry recognized certifications strategically into education/higher education/training programs of study.
6. Blend, align, and link cybersecurity education and workforce development programs into key pathways supporting strategically important “high demand/hard to fill” NICE Cybersecurity Framework 2.0 work roles;
7. Call to action to cybersecurity key partners and major stakeholders to collaborate and build and support cybersecurity career education pipelines and pathways to reduce current and future critical workforce capability and skill gaps.

SECTION #1

Cybersecurity Workforce Development and Education (WDE) Challenges, Problems, Barriers, Obstacles, and Limitations

Cybersecurity workforce and labor shortages pose a critical national and economic security. The specter of global political tension, uncertainty and conflict provide motivations for attacks on critical infrastructure, organizations, and individual data and privacy. Major factors driving cyber workforce development and education capability gaps is often found in domain technical complexity, uneven access to education and training, and the "siloization" of key stakeholders and major partners in this ecosystem. In addition, there is a significant learning curve for cybersecurity jobs, including for entry level work roles.

One first step of the ATARC Working Group process was to develop a deeper understanding of the challenging nature of cybersecurity Workforce Development and Education (WDE). These pressing issues are addressed in this report section on cybersecurity WDE challenges, problems, barriers, obstacles, and limitations that contribute to national and state workforce capability and skills gaps. There are several specific challenges to cybersecurity WDE. One significant obstacle and barrier to cybersecurity workforce preparation is found in the steep learning curve within the professional field. Cybersecurity is a subfield of IT and can be very technical. It utilizes various skills, competencies, levels of proficiency, and many different workforce roles. Without an appropriate higher education background, industry recognized professional certifications, training, and job experience, getting into the field is difficult.

While many available positions exist, there is also a growing number of people interested in the field. However, they may not understand how to get into the field and what they may need in the preparation process. This would be accomplished by way of the implementation of a comprehensive cybersecurity career pipeline/pathway and accompanying road map into the profession. These are examples of some of the cybersecurity workforce development and education challenges that we must overcome by way of a clearly articulated cybersecurity career education pipeline/pathway and accompanying roadmap.

This report studies and evaluates five types or categories of barriers, obstacles, and limitations in current cybersecurity education, training, and workforce development practices:

Cybersecurity education and workforce development challenges are divided into five categories below. The first category includes the broader “big picture” structural issues found within current cybersecurity education and workforce development preparation practices, policies, and processes. Four additional categories focus on narrower issues impacting key actors and major partners within the Cyber WDE ecosystem. Challenges are summarized below and a detailed discussion to follow.

Summary of Cybersecurity Workforce Development and Education Challenges

Significant challenges exist in cybersecurity workforce development and education. These challenges are analyzed in terms of broader themes and underlying structural issues. However, we also dig deeper to analyze challenges respective to the needs and perspectives of diverse key stakeholders and major partners found within this ecosystem. These include the public sector, private sector, academia (K-12 & Higher Education), and Community Based Organizations (CBOs).

1. "Big Picture" Cybersecurity Workforce Development & Education Structural Issues-
2. Private Sector-
3. Public Sector-
4. Academia- (K-12 and Higher Education)
5. Community/neighborhood-based Organizations/NFPs/ NGOs-

Cybersecurity Workforce Development and Education Challenges

1. "Big Picture" Strategic barriers, obstacles, and limitations in current cybersecurity education, training, and workforce development: Structural issues.
    - Diversity issues in IT-Cyber. Recruiting, hiring, getting into the field; race, gender, age, neurodivergent workforce, geographical regions, etc.
    - How to weave students into professionals: cyber teams—as a solution to state-level cybersecurity WDE; mentoring for success in the professional field.
    - Science, Technology, Engineering, and Mathematics (STEM)/STEAM.
    - Balancing study and work- both as job requirements and as a strategy for time management.
    - Synch and pacing of a rapidly evolving industry looking for specialized and skilled job candidates; we need to make sure that HR standards support job preparation, the recruiting and hiring processes, and employee workplace retention.

Structural Challenges and Solutions:

1. Cybersecurity strategic planning with an eye on development, implementation, and scalability, "How to grow and enhance education, training, and workforce development."
2. Strengths, Weaknesses, Opportunities, and Threats (SWOT) Analysis; Strategic discipline formation; Fundamentals of threats and strategic solution seeking.
3. Lacking key cybersecurity educational infrastructure on many school, college, and university campuses. This includes resources, classroom space, labs, faculty, instructional materials, cyber-ranges, etc. Some educational institutions are better situated than others in promoting emerging technologies. We need to do a better job of understanding infrastructure needs to fill educational institutional capability and skills gaps. Elevate more participating campuses and programs.
4. Marketing, recruiting, and sustaining of students and prospective professionals into the field. We have many fields within the cybersecurity profession. This is a challenge in the

profession with many different NICE Cybersecurity Work roles to include in a cybersecurity pipeline/pathway education and workforce preparation process.

5. How do we simplify the program and not turn students off from the field? STEM, Computer Science and Engineering have similar issue relating to relatability, accessibility, appropriate mathematics background, and this is one reason why interesting IT-cybersecurity gamification and content is so important. These maintain student interest while they are learning cybersecurity foundational knowledge and the "fundamentals." Some critics consider Introductory cyber to be “boring". We need to make it more fun and exciting!
6. Cybersecurity Programs and courses are very technical on the front end. Make the courses “user friendly” (and interesting) by utilizing activities, tools, and mixed-media teaching materials through strong introduction course design and development principles.
7. Importance of the “Earn and Learn” workforce development including Registered Apprenticeships (with a 1 year/ 2000 hours On the Job Training) and Internships (short term) cybersecurity workforce development and education opportunities.
8. Diversity, equity, accessibility, and inclusivity in cyber education/workforce development.

Cybersecurity Key Stakeholders and Major Partner Challenges

Public Sector Challenges

1. Public sector salaries are not competitive with private sector colleagues. This impacts State, Local, Municipal, Special Districts, and Education Sector employer hiring and retention.
2. Poaching and talent acquisition issues. The public sector does not typically pay as well as private sector counterparts. There is a significant retention issue to compete with private sector employers when extensive employee salary differentials exist between sectors.
3. Significant 4-Year degree requirements for public sector cyber positions.
4. Resources may be hard to come by to find and retain top cybersecurity talent.

Private Sector Challenges

1. The pace of innovation in emerging technologies is dynamic. It is difficult for workforce education and training to keep up with this accelerated pace with salient curriculum, content, skills, and tools. The question becomes, “How to build (and routinely update) cybersecurity education and workforce development programs to meet current talent acquisition needs (i.e. knowledge, skills, competencies) for prospective employers?” This challenge is resolved in part through engagement, collaboration, coordination, and curriculum development with key partners.

2. Challenges remain with the preparation level, quality, and cost of prospective job candidate education and training. This is a cycle. Industry needs to know that students are qualified and prepared with the skills, tools, and competencies to contribute to the workplace from day one; not that new hires "require" significant additional training to get them up to speed to meet workplace needs. Also, the question of employees securing the appropriate industry recognized professional certifications necessary for various work roles.

3. How do you utilize agile implementation (and flexibility) for evolving skills and tools used within the profession as this changes rapidly over time?

4. Entry level, intermediate, and advanced roles– and the role of support throughout the career ladder from recruiting, to hiring, and retention. It is hard for employers to justify significant training costs when talent may leave the position after a few months on the job.

5. When seeking qualified cybersecurity workforce, we need to discuss variations across critical infrastructure sectors in the economy. Specific industry sector cybersecurity employee needs are not the same and should not be treated as such. Presidential Directive 8- (PPD-8) lays out national critical infrastructure sectors. These critical industry sectors (and additional key information) are found at the following link:

   https://www.dhs.gov/presidential-policy-directive-8-national-preparedness

6. Regional impact on cybersecurity workforce development and education preparation and work role availability: Educational institutions and jobs are local/regional matters.

Academia Sector Challenges

1. Quick speed of technology and digital innovations. Glacial speed of program and course curriculum development, approval, and updating (keeping up to date regularly.

2. Do cybersecurity education programs meet the current needs of industry (i.e. employers)?

3. Collaboration, advisory boards; getting stakeholders– “good offices” to facilitate the conversation, strategic communication, and working together to prepare skilled job candidates.

4. How do we strengthen campus and workforce opportunities for students and our campuses– campus employment with technology services? Student run SOCs?

5. Emphasis on practical experience and help build model programs where students can work with campus cybersecurity initiatives; like campus SOCs for example.

6. Find ways to encourage partnership with cybersecurity service providers for offering student internships as a criterion for SLED contracts.

7. Diversity of University/College academic disciplines– all college majors are of value to the many varied perspectives (and work roles!) found within the IT-Cybersecurity ecosystem. More cyber students are now found outside of Computer Science programs, also Engineering, Info Sciences, Business Schools, Education, Social Sciences, Liberal Arts, Law Schools, etc.

8. Diversity of modality for education/training- involve educational institutions with bootcamps, academies, and video technology. Diversity is an important element teaching and learning and how we help people see themselves in the cybersecurity enterprise.

9. Taxonomy of cyber challenges, needs, and potential solutions– based on NICE work roles/duties.

10. General Education (GE) courses– the need for cyber awareness courses across campus.

11. Cyber education covers all levels of education and feeders from K-12 before going on to college.

    - Soft start cyber education: how do we bring individuals with no tech skills or cyber Embed education/training with work experience opportunities like apprenticeships.

12. Students have degrees but no cyber jobs. We must focus on the critical importance and value of work experience opportunities like internships and apprenticeships. Get students involved in the work/application process so they know how to effectively communicate their knowledge, skills, and abilities to prospective employers.

13. Career advising and mentoring; *The Value of a* Cyber Education, Training, and Workforce Development Career Roadmap–

14. Lacking academic standards, standardized curriculum, and accreditation/accrediting bodies.

Community-Based/ Neighborhood Organizational Challenges

1. One barrier, obstacle, and limitation in the tech field is a lack of diversity and inclusivity of women and under-represented groups in the IT-Cybersecurity field.
2. We need to do a better job as a professional field to reach out and into communities that tech has not always served very well when looking to recruit and hire from.

3. A security perspective is enhanced when viewed from many different lenses. A failure to develop effective STEM-Cybersecurity strategies for diversity and inclusivity is a significant barrier to reducing current critical cybersecurity workforce gaps.
4. The value and benefit of enhancing Diversity, Equity, Inclusivity and Accessibility (DEIA) and working with local and community-based and neighborhood organizations to increase awareness and WDE programs and opportunities nation-wide.
5. Under-resourced relative to the community's need for WDE in emerging technologies like AI and cybersecurity.

Section 1 Conclusion

There are numerous challenges and issues that limit and constrain cybersecurity workforce development and education nationally. Some of these challenges are structural and apply across the country. Other challenges vary across key stakeholders and major partners including public sector, private sector, academia, CBOs, and local neighborhood groups. Each group of stakeholders has their own unique perspective on the nature and impact of these issues. Now that we have a better understanding of these broader issues and the significance of the key issues in cybersecurity workforce development and education, we discuss eight report sections that comprehensively address each critical and interrelated area. The first area for discussion and recommendations is on securing K-12 and Higher Education digital critical infrastructure protection. After all, it is difficult to teach, learn, research, and provide workforce development in an "unsecured environment" fraught with numerous cybersecurity vulnerabilities and risks including ransomware, malware, cyber-bullying, and loss of privacy. As many know, K-12 Education, Colleges, and Universities are one of the most visible targets of ransomware and malware attacks. Campus preparedness and awareness problems and solutions are the theme of Section 2.

SECTION #2

Framework and Strategies for Hardening Campus Information Security & Networks; Campus Critical Infrastructure Protection & Digital Awareness Programs

Prepared by:

Gregory W. Cooper, Information Systems Operations Center (ISOC) Manager, New Mexico State University Physical Science Laboratory

Eric Wall, Chief Information Security Officer, University of Arkansas System

Section 2 Overview

This comprehensive section delves into the strategic integration of established cybersecurity frameworks with strategies aimed at hardening campus information security, protecting critical infrastructure, and enhancing digital awareness across educational institutions. Recognizing the multifaceted nature of cybersecurity challenges in the educational sector, this section outlines a holistic approach to leverage structured guidance provided by cybersecurity frameworks, while also addressing the specific needs and vulnerabilities of educational environments.

Key components in this section

1. Adoption of Cybersecurity Framework(s): Begins with an exploration of leading cybersecurity frameworks such as NIST 800-171 and NIST 800-53, highlighting their principles, practices, and how they can be tailored to the unique contexts of educational institutions and how they relate to relevant higher education laws.

2. Hardening Campus Information Security and Networks: Offers detailed strategies for enhancing network security, including the deployment of advanced cybersecurity measures like firewalls and intrusion detection systems, network segmentation, secure Wi-Fi practices, and the importance of data encryption and regular backups. The focus is on aligning these strategies with the broader objectives outlined in the chosen cybersecurity framework(s).

3. Protecting Campus Critical Infrastructure: Discusses the importance of safeguarding both physical and digital infrastructure essential to the institution's operations. It emphasizes conducting regular risk assessments, developing emergency response and business continuity plans, and how these efforts are supported and structured by cybersecurity frameworks.

4. Enhancing Digital Awareness and Literacy: Covers the development and implementation of comprehensive digital literacy programs that integrate seamlessly with cybersecurity education and practices as recommended by cybersecurity frameworks. This includes curriculum integration, professional development for

educators, and fostering a campus-wide culture of cybersecurity awareness and responsibility.

Framework Introduction: Primary Driving Standard

Educational systems, such as K-12 and Universities, are complex large organizations with some being the equivalent of small cities. As with all business entities, they have limited resources and demands always exceed the resources they have. Some of those demands, which are also legally required, are information protection standards mandated by the government. There are many of these standards, all depending on the data source, what the data is, and/or what the data represents. Some examples are HIPAA, GLBA, FERPA, SOX, PCI-DSS, and CMMC. Adding to that, the budgeting for protecting information historically has been lacking. Therefore, it is imperative that these educational systems find ways to be efficient with the funding for information security they do have to allocate.

The goal of this paper is to introduce an actionable mechanism for educational systems to meet the government's requirements while using less resources. That mechanism would be selecting a Primary Driving Standard from the list of required standards that the organization must implement. The standard selected will be the Primary Driving Standard (PDS) for that entity.

Primary Driving Standard Framework Process

The goal of the framework is to reduce the burden of maintaining compliance across the myriad of standards required yet meeting those standards. In short, select the most detailed/rigorous standard as the Primary Driving Standard (PDS) that the organization is required to implement, then crosswalk the other standard's controls against the selected PDS. If none of the standards on the organizations list are adequately rigorous then a higher, or more rigorous, standard could be selected as the PDS. The intent is to select a standard that meets more than 80 - 90% of the controls across all of the other standards.

Let us jump right into an example to determine a PDS for an institution. GLBA has recommended adopting NIST 800-171 as the standard to meet the obligations under GLBA. An excerpt below from the Office of Federal Student Aid in their electronic announcement ID: GENERAL-23-09 "Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements"

> *"In Dear Colleague Letters GEN-15-18 and GEN-16-12, we reminded institutions about the longstanding requirements of GLBA and notified them of our intention to begin enforcing the legal requirements of GLBA through annual compliance audits. In Dear CPA Letter CPA-19-01, the Office of Inspector General (OIG) explained the audit procedures for auditors to determine whether institutions were complying with GLBA. On February 28, 2020, we issued an Electronic Announcement that explained the Department's procedures for enforcing those requirements and the potential consequences for institutions or servicers that fail to*

comply. On December 18, 2020 we issued an Electronic Announcement encouraging institutions to review and adopt NIST 800–171 as a security standard to support continuing obligations under GLBA."

Those requirements went into effect on June 9, 2023. So if your institution has a GLBA requirement then NIST 800-171 is added to your list of required standards. If your institution will also be handling CUI, then NIST 800-171 is again the required standard.

Privacy of student education records is found under the FERPA law (Family Educational Rights and Privacy Act). FERPA mandates that student records are protected but does not reference a control set. So, some care is going to be needed when selecting the controls that will be implemented. An institution could select NIST 800-53, a very rigorous standard, for the controls, and publications can be found that have a crosswalk from NIST 800-53 to FERPA. Some institutions may be implementing NIST 800-53 due to other constraints, such as the protection of federal classified information (otherwise known as National Security Systems). But in most cases NIST 800-53 is implemented in a very contained area and not campus wide due to the enormous cost. NIST 800-171 could also be mapped to the FERPA requirements if NIST 800-53 is beyond the reach of the institution. Remember, the goal here is to find a standard that can be implemented campus wide and woven into the culture.

Special Note to Congress: When creating the laws that cover a cyber implementation to protect data, allow for higher or more rigorous standards to be acceptable as a replacement for the named standard. This can be passed down to the accrediting/oversight body to name the acceptable PDS standards. By doing so, Congress will not need to rewrite the law as new standards become mainstream, combatting the ever-changing landscape of network attacks.

Table 2: Possible Primary Driving Standards for Current Cyber Laws

Law	Named Standard	Possible PDS Standard
GLBA	NIST 800-171	NIST 800-171, NIST 800-53
CMMC	NIST 800-171	NIST 800-171, NIST 800-53
FERPA	None	NIST 800-171, NIST 800-53
FISMA	NIST 800-53	NIST 800-53
HIPAA	None	NIST 800-66, NIST 800-171, NIST 800-53
PCI-DSS	PCI-DSS	NIST 800-171, NIST 800-53
SOX	None	COSO, COBIT, NIST 800-171

The end goal of implementing the PDS is twofold; provide an evidence-based and consistent implementation of a single standard throughout the IT infrastructure as well as provide IT resiliency. IT resiliency is the organization's ability to continue providing services to its legitimate customers while adapting to attacks, software updates, disruptions, hardware failures, disasters, power loss, and any other event that can degrade information systems from performing as designed. Resiliency can be broken into these groupings:

- Cybersecurity: create a Security Operations Center (SOC), also known as an Information Security Operations Center (ISOC), Security Defense Center (SDC), Security Analytics Center (SAC), or Network Security Operation Center (NSOC) to audit the network and provide risk analysis to management.
- Continuous Monitoring: the SOC should be providing continuous monitoring of the controls implemented. Several controls in the NIST 800-171 and NIST 800-53 specifically require monitoring. Does that monitoring provide alerts when something defined or unexpected occurs?
- Backups: is critical data being backed up with a frequency consistent with accepted risk. Are those backups being tested and proven they can be restored as expected?
- Disaster Recovery: does the organization have a disaster recovery plan? Is it specific enough to use during an actual event? Has that plan been tested?
- Redundancy: backups are not enough. When a critical server or system fails, restoring the data to another system may not be adequate. Does the organization have redundancy of hardware and/or systems to recover? Example: an access control system is hardware based and just having backups of the database does not provide resiliency. If the controller fails, the data is practically meaningless.
- Fault Tolerance: can systems be implemented that adjust to negative impacts automatically?
- Testing: how often does all of the above get tested? Are adjustments made when tests do not come out as expected? I am a big proponent of un-planned testing. As the ISOC manager, if I announce that I am going to kill power to the data center and verify that all of the UPSes and the power generator are working as expected, then amazingly the IT department begins to verify that the UPSes have a good charge, and the generator has fuel, and an email goes out to employees that there may be a data disruption in the next hour. Mother Nature does not always keep us posted when power failure is imminent. Therefore, weave unplanned testing into your processes wherever possible.

These must become part of the IT and ISOC culture. Promulgating the practices you want to implement becomes a paramount objective. Not only do they need to be adopted, but they also need to become so ingrained into the organization that each employee is always thinking about building in resiliency as they design systems.

Promulgating the culture change can include:

- Tools and Resources: such as checklists, guides, websites, and outlines that help your employees get their job done easier. If you come across best practices, post them regularly.
- Join Professional Organizations: being part of a professional organization allows for sharing issues as well as grievances. Finding out that other companies are experiencing the same challenges actually helps moral and finding creative solutions that may become industry standards later.
- Training: of course there is always training. But something interesting that I find becoming more prevalent is electronic badges for completing a training or a set of trainings that become part of the employee's profile.
- Feedback: getting feedback from your customers, and actively asking for it, goes a long way for those same customers to have tolerance when things are going sideways.
- Metrics: measuring how you are doing today and then comparing that to how you are doing a year later makes every employee feel that they are either succeeding or not. Though it takes a long time, it also provides strong internal incentives to do better and everyone feels it together.
- Incentives: recognition goes a long way in driving the implementation of best practices. And it doesn't have to be significant or monetary for that matter. For many people, simple recognition for a job well done is incredibly meaningful.

As we transition from the discussion on cybersecurity frameworks and their critical role in shaping robust security strategies for educational institutions, it becomes imperative to explore how these frameworks can be practically applied and integrated within the specific context of campus security and digital literacy efforts. This segue leads us into a detailed examination of targeted strategies for hardening campus information security, protecting critical infrastructure, and enhancing digital awareness programs. By bridging the gap between the theoretical underpinnings of cybersecurity frameworks and the tangible actions educational institutions can undertake, we aim to provide a comprehensive blueprint. This blueprint will not only align with best practices and standards outlined by such frameworks but also address the unique challenges and needs of educational environments. The following sections delve into the specifics of implementing advanced cybersecurity measures, safeguarding essential infrastructure, and cultivating a pervasive culture of digital literacy and safety – all within the framework-guided approach to cybersecurity.

Educational institutions globally are undergoing a seismic shift towards digitization. This transformation, accelerated by the increasing reliance on online learning platforms and digital administrative systems has rendered cybersecurity and network integrity paramount in both K-12 and higher education sectors. As these institutions become repositories of vast amounts of

sensitive data and continue to integrate technology into every facet of their operations by digitizing their repositories, they face an escalating risk of cyber threats. This evolving landscape necessitates a comprehensive approach to securing digital infrastructure, protecting critical assets, and enhancing digital literacy among all stakeholders. This section aims to provide actionable insights and strategies to address these challenges, ensuring that educational institutions not only adapt to the digital age but thrive securely and resiliently within it.

In the contemporary era, where digital technology pervades every aspect of our lives, the significance of robust information security and network integrity in educational institutions cannot be overstated. Educational entities, encompassing K-12 schools and higher education institutions, are increasingly reliant on digital platforms for a myriad of functions ranging from administrative operations to academic processes. This shift towards a digital-centric modus operandi, while beneficial in numerous ways, has also exposed these institutions to a spectrum of cyber threats and vulnerabilities.

The necessity to fortify the digital infrastructure of educational institutions is not just a matter of safeguarding data; it is integral to preserving the integrity of educational processes and the privacy of students and staff. Cybersecurity threats such as data breaches, ransomware attacks, and network intrusions pose significant risks. These risks are not limited to the loss or compromise of sensitive data but also include potential disruptions to the educational process, financial losses, and damage to the institution's reputation.

The objective of this section is to delve into the intricacies of hardening campus information security and networks, protecting critical infrastructure, and enhancing digital awareness in the context of K-12 and higher education settings. The discussion is premised on the understanding that cybersecurity is not a static goal but an ongoing process that involves continuous evaluation and adaptation to new threats. The section outlines specific actions that can be implemented to strengthen these areas, thereby contributing to the overall robustness and efficiency of educational infrastructures.

The digital landscape within educational environments is complex and multifaceted. It encompasses a wide array of technologies and platforms, including but not limited to student information systems, learning management systems, email and communication platforms, and the broader campus network infrastructure. The integration of these systems into the daily operations of educational institutions means that the impact of cyber threats can be widespread, affecting every aspect of educational administration and delivery.

Furthermore, the diverse user base within educational institutions adds another layer of complexity to cybersecurity efforts. Students, faculty, and administrative staff all interact with the institution's digital systems, often with varying levels of technical expertise and cybersecurity awareness. This diversity necessitates a multifaceted approach to cybersecurity, which not only focuses on technological solutions but also emphasizes the importance of user education and awareness.

The first part of this report section will focus on strategies for hardening campus information security and networks. This includes the deployment of advanced cybersecurity measures such as firewalls and intrusion detection systems, regular software updates and patch management, network segmentation, secure Wi-Fi networks, data encryption, and regular data backups. The discussion will also delve into the specific challenges and solutions relevant to educational institutions, recognizing the unique environment they operate in.

The second part will explore the protection of critical infrastructure within educational settings. This includes conducting regular risk assessments to identify potential threats and vulnerabilities, developing and implementing risk mitigation strategies, and establishing emergency response and continuity planning. The focus will be on both physical and cybersecurity measures, acknowledging the interconnectivity between these two domains in protecting critical infrastructure.

The final part will address the enhancement of digital awareness programs. This encompasses developing comprehensive digital literacy programs that are integrated into the curriculum, providing professional development for educators, conducting awareness campaigns and workshops, and engaging students in cybersecurity initiatives. The section will highlight the importance of creating a culture of cybersecurity within educational institutions, recognizing that technological solutions alone are insufficient to address the myriads of cyber threats.

In conclusion, this expanded introduction sets the stage for a detailed exploration of the strategies and actions necessary for enhancing the cybersecurity posture of educational institutions. By addressing the technological, procedural, and educational aspects of cybersecurity, this section aims to provide a comprehensive guide for educational institutions seeking to navigate the complex landscape of digital threats and opportunities.

Part I - Strategies for Hardening Campus Information Security and Networks

The Digital Landscape in Education: An Overview

In the current educational landscape, digital technology plays an indispensable role. The transition from traditional teaching methods to digital platforms, accelerated by global trends such as the COVID-19 pandemic, has significantly altered how educational institutions operate. This shift has made information security and network integrity crucial components of a school's infrastructure.

Unique Cybersecurity Challenges in Educational Institutions

Educational institutions face distinct challenges in securing their networks:

1. Diverse User Base: Schools and universities cater to a broad audience, including students, faculty, and administrative staff, each with varying levels of digital literacy and access needs.

2. Wide Range of Devices: The integration of various devices, such as laptops, tablets, and smartphones, into educational networks increases complexity and vulnerability.
3. Open Access vs. Security: Educational institutions traditionally foster open access to information. Balancing this with the need for robust security measures is a unique challenge.

Evolving Cyber Threat Landscape

The cyber threat landscape has evolved rapidly, with educational institutions becoming prime targets for cyber-attacks. These threats range from data breaches and ransomware attacks to more sophisticated nation-state-sponsored espionage, particularly targeting research data in higher education institutions. The consequences of these incidents can be severe, including loss of sensitive data, financial losses, legal ramifications, and damage to the institution's reputation.

Need for a Holistic Security Approach

Given these challenges, there is a critical need for a holistic approach to cybersecurity that encompasses not only technological solutions but also involves policy formulation, user education, and a shift in organizational culture towards prioritizing digital security.

Primary Objectives in Hardening Network Security

The primary objectives for hardening campus information security and networks include:

1. Protecting Sensitive Data: Ensuring the confidentiality, integrity, and availability of sensitive information, including student records, financial information, and intellectual property.
2. Maintaining Network Integrity: Guaranteeing that the network is available and resilient to attacks, ensuring that educational and administrative functions can proceed uninterrupted.
3. Ensuring Compliance: Complying with legal and regulatory requirements, such as FERPA in the United States, which mandates the protection of student educational records.

Deploying Firewalls and Intrusion Detection Systems

In the realm of campus network security, the implementation of current-gen firewalls and Intrusion Detection and Prevention Systems (IDS/IPS) stands as a primary line of defense. Firewalls serve to monitor and control the incoming and outgoing network traffic based on an applied set of rules, thereby creating a barrier between secure internal networks and untrusted external networks. The customization of firewall rules is crucial for educational institutions to balance the need for security with the requirement for academic freedom and information accessibility.

Intrusion Detection and Prevention Systems complement firewalls by monitoring network traffic for suspicious activity and potential breaches. IDS/IPS can be configured to alert network administrators of abnormal patterns or known attack signatures, allowing for rapid response to potential threats. The effectiveness of IDS/IPS in educational institutions lies in its ability to provide real-time monitoring and alerting without disrupting the normal flow of network traffic.

Regular Software Updates and Patch Management

Another cornerstone of a robust cybersecurity strategy is the maintenance of up-to-date software and diligent patch management. This practice is critical because many cyber-attacks exploit vulnerabilities in outdated software. Educational institutions often operate a wide range of software applications, making consistent updates a complex task.

Implementing a systematic approach to software updates and patch management is essential. This includes establishing regular schedules for checking and applying updates, prioritizing patches based on the severity of the vulnerabilities they fix, and ensuring that all devices connected to the network are covered under this regime. Automated patch management tools can aid in this process, especially in larger institutions, by ensuring that all systems are consistently and promptly updated.

Challenges and Best Practices

- Balancing Access and Security: One of the primary challenges in implementing these measures in educational settings is balancing the need for an open and accessible network with security imperatives. This balance requires a nuanced approach to firewall configuration and IDS setup, ensuring that security measures do not unduly restrict academic activities.
- Managing Diverse Systems: Given the diverse range of software and hardware used in educational institutions, establishing a comprehensive and efficient patch management system can be challenging. It requires a thorough inventory of all assets and a clear understanding of the network architecture.
- Continuous Monitoring and Response: With the deployment of IDS, it is crucial to have a dedicated team for continuous monitoring and rapid response to detected threats. This team should be equipped with clear procedures for incident response and mitigation.

Network Segmentation: Isolating Risks to Enhance Security

Network segmentation plays a pivotal role in enhancing the security of campus networks. By dividing the larger network into smaller, more manageable segments, institutions can contain and isolate cybersecurity threats, preventing them from spreading across the entire network. This strategy is particularly effective in environments like educational institutions, where many users access the network for a variety of purposes.

Segmentation can be implemented in several ways, such as creating separate networks for different departments, segregating student, and staff networks, or isolating critical systems like financial and research data from the general campus network. This approach not only improves security but also enhances network performance and management.

Challenges in Implementing Network Segmentation

- Complexity of Network Design: Properly segmenting a network requires a deep understanding of the institution's network architecture and the specific needs of different user groups.
- Maintaining Accessibility: It is crucial to ensure that network segmentation does not hinder the accessibility of resources needed for educational and administrative purposes.
- Continuous Monitoring and Maintenance: Segmented networks require ongoing monitoring and maintenance to ensure they remain secure and function as intended.

Securing Wi-Fi Networks: Ensuring Wireless Security

Wi-Fi networks in educational institutions are often susceptible to various security risks, including unauthorized access and data interception. Securing these networks is crucial, as they are widely used by students and faculty for educational and personal purposes.

Implementing the latest Wi-Fi security protocols, such as WPA3, is a fundamental step. These protocols provide robust encryption, which helps in safeguarding data transmitted over wireless networks. Additionally, regular monitoring of Wi-Fi networks for unauthorized access points and devices is essential to prevent unauthorized access and potential network breaches.

Challenges in Securing Wi-Fi Networks

- Wide Coverage and High User Density: The extensive coverage and high user density of Wi-Fi networks in educational settings make them challenging to secure.
- Balancing Ease of Access with Security: Institutions must balance the need for easy access to Wi-Fi networks for legitimate users with the need to secure these networks against unauthorized access.
- Education and Awareness: Users of Wi-Fi networks must be educated about best practices in network security, such as the importance of using secure passwords and avoiding unsecured networks.

Data Encryption: Safeguarding Sensitive Information

Data encryption is a fundamental aspect of protecting sensitive information within educational institutions. This process involves converting data into a coded format that can only be accessed with a specific key or password, thus safeguarding it from unauthorized access, both in transit over the network and at rest in storage systems.

The importance of encrypting sensitive data cannot be overstated, especially in educational settings where personal information of students, staff, and faculty, as well as sensitive research data, are routinely handled. Encryption methods such as AES (Advanced Encryption Standard) are widely recommended for their robustness.

Challenges in Implementing Data Encryption

- Comprehensive Coverage: Ensuring that all sensitive data, regardless of where it is stored, transmitted, or encrypted, can be challenging, particularly in large/diverse network environments.
- Key Management: Effective key management is critical to the success of encryption efforts. Lost or improperly managed keys can render encrypted data inaccessible.
- Balancing Performance and Security: Encryption can impact system performance, so finding the right balance between security and usability is essential.

Data Backup: Ensuring Data Resiliency

Regular and secure data backups are crucial for any institution, especially in educational environments where data loss can have far-reaching consequences. An effective data backup strategy involves regularly copying and storing data in multiple locations, including off-site or cloud storage, to prevent data loss due to system failures, cyber-attacks, or natural disasters. Adopting a “bunker in a box” strategy that offers both immutability and indelibility are critical pieces of ensuring that you can recover.

Backup strategies should include not only the backing up of critical data but also regular testing of backup systems to ensure data integrity and the ability to restore systems quickly in the event of a loss.

Challenges in Effective Data Backup

- Regular and Consistent Backups: Establishing a routine for regular and consistent backups can be challenging, especially in ensuring that all critical data is included.
- Data Recovery Plans: In addition to backing up data, institutions need to have clear and tested plans for data recovery. This ensures minimal downtime in case of data loss.

- Security of Backup Data: Backed-up data is also vulnerable to cyber threats and needs to be protected with the same rigor as primary data, including the use of encryption and secure storage solutions.

Part II - Protecting Campus Critical Infrastructure

Defining Critical Infrastructure in the Educational Context

Critical infrastructure in educational institutions encompasses a wide range of assets that are essential for their operation and resilience. This includes physical elements like buildings, laboratories, power systems, and technological components such as servers, network hardware, and databases. The protection of this infrastructure is crucial, as any disruption can have significant implications for the continuity of educational services, research activities, and overall campus safety.

Emerging Threats to Critical Infrastructure

The threats facing critical infrastructure in educational settings are diverse and evolving. They range from natural disasters and physical attacks to sophisticated cyber threats targeting data systems and network infrastructure. Cyber threats, in particular, have become more prevalent, with institutions facing risks like ransomware attacks, data breaches, and disruptions to network services. These threats can compromise student and staff data, disrupt academic and administrative activities, and lead to substantial financial and reputational damage.

Interconnected Nature of Modern Infrastructure

Modern educational infrastructure is highly interconnected, with physical and digital systems often intertwined. For instance, access to buildings may be controlled by digital systems, while teaching and learning increasingly relies on digital platforms. This interconnectedness means that a breach in one area can have cascading effects across the institution.

The Need for a Comprehensive Protection Strategy

Given the complex nature of these threats and the interconnectedness of infrastructure, it's clear that a comprehensive strategy is needed to protect these critical assets. This strategy must encompass both physical security measures, such as secure campus environments and emergency response plans, and cybersecurity measures, including network security and data protection protocols.

Prioritizing Infrastructure Security

Prioritizing the security of critical infrastructure is essential for maintaining the operational integrity and safety of educational institutions. It involves not just the implementation of

security measures but also regular risk assessments, staff training, and the development of incident response and recovery plans.

Identifying Risks

Conducting Regular Risk Assessments

Regular risk assessments are vital for understanding and managing the threats to critical infrastructure in educational institutions. These assessments involve identifying potential hazards, assessing the vulnerabilities of physical and digital assets, and evaluating the potential impacts of these threats. This process should be systematic and ongoing, reflecting changes in the threat landscape and the evolution of the institution's infrastructure.

Key Components of Risk Assessments

1. Identifying Threats: This involves recognizing potential sources of harm, including natural disasters, technological failures, and human-caused threats like cyber-attacks or vandalism.

2. Assessing Vulnerabilities: This step evaluates how susceptible the institution's infrastructure is to identifying threats. It considers factors like the age and condition of physical infrastructure and the robustness of cybersecurity measures.

3. Impact Analysis: Understanding the potential consequences of various threats helps prioritize risk management efforts. Impact analysis considers factors such as the severity of potential damage and the likelihood of different types of incidents.

Developing and Implementing Risk Mitigation Strategies

Once risks are identified and assessed, the next step is to develop and implement strategies to mitigate these risks. This involves a combination of preventive measures and contingency planning.

1. Preventive Measures: These are steps taken to reduce the likelihood or impact of an incident. For physical infrastructure, this might include enhancing building security or reinforcing structures against natural disasters. In the digital realm, it might involve strengthening cybersecurity defenses or improving network resilience.

2. Contingency Planning: Despite the best preventive measures, some risks cannot be eliminated entirely. Contingency planning involves preparing to manage and minimize the impact of incidents that do occur. This includes developing response plans, establishing backup systems, and training staff in emergency procedures.

Challenges in Risk Assessment and Management

- Dynamic Threat Landscape: The constantly evolving nature of threats, particularly cyber threats, makes risk assessment and management an ongoing challenge.
- Resource Constraints: Limited resources can restrict the ability to implement comprehensive risk mitigation strategies, especially in smaller institutions.
- Stakeholder Involvement: Effective risk management requires the involvement of various stakeholders, including faculty, staff, students, and possibly external partners. Coordinating these efforts can be complex.

Emergency Response and Continuity Planning

The Imperative of Emergency Response Planning

In the context of safeguarding critical infrastructure in educational institutions, having a robust emergency response plan is imperative. Such plans are essential not just for addressing immediate threats or disruptions but also for ensuring the rapid resumption of educational and administrative functions post-incident. These plans should be comprehensive, covering a range of potential scenarios including natural disasters, technological failures, and security breaches.

Components of an Effective Emergency Response Plan

1. Incident Identification and Assessment: Quick and accurate identification of an incident's nature and scope is critical. The plan should outline procedures for assessing the severity and potential impact of the incident.
2. Communication Protocols: Clear communication channels and protocols are essential. This includes internal communication with staff and students, as well as external communication with law enforcement, emergency services, and potentially the media.
3. Roles and Responsibilities: Clearly defined roles and responsibilities ensure an organized and effective response. This includes designating a response team and outlining specific actions for various staff members.
4. Evacuation and Safety Procedures: In cases of physical threats, well-practiced evacuation and safety procedures are vital to ensure the safety of all campus occupants.
5. Resource Allocation and Management: Efficient allocation and management of resources, such as emergency supplies, technology, and personnel, are essential during a crisis.

Business Continuity and Disaster Recovery Plans

Beyond immediate response, institutions must also have plans for continuing their essential functions in the aftermath of a disruption. Business continuity and disaster recovery plans focus

on restoring critical functions and minimizing the impact of a disruption on the educational process.

Key Aspects of Continuity Planning

1. Identification of Critical Functions: Determining which functions are critical to the institution's operation, such as teaching, research, and student support services.
2. Backup Systems: Implementing backup systems, especially for critical digital data and infrastructure, to ensure continuity in the event of system failures.
3. Alternative Operations Plans: Developing plans for alternative modes of operation, such as remote teaching and administrative work, in situations where the campus is inaccessible.

Challenges in Emergency Response and Continuity Planning

- Complexity of Scenarios: Planning for a wide range of potential incidents, each with its unique challenges, can be complex.
- Regular Updating and Testing: Plans must be regularly updated to reflect new threats and changes in the institution's infrastructure. Regular drills and tests are essential to ensure preparedness.
- Stakeholder Involvement: Involving all stakeholders, including faculty, staff, and students, in emergency response and continuity planning is crucial, but also challenging in terms of coordination and communication.

Part III - Enhancing Digital Awareness Programs

Understanding the Digital Landscape in Education

In the current era, digital literacy is not just a skill but a fundamental requirement for participating effectively in the educational environment. With the increasing integration of digital technology in education, from online learning platforms to digital administrative systems, the need for comprehensive digital awareness and literacy programs is more pronounced than ever. These programs are essential not only for enhancing the educational experience but also for safeguarding the digital ecosystem of educational institutions.

The Significance of Digital Literacy in Educational Settings

Digital literacy extends beyond the ability to use technology; it encompasses understanding how to navigate the digital world safely and responsibly. In educational institutions, this includes awareness of cybersecurity threats, understanding data privacy, and the ability to discern reliable from unreliable digital content.

1. Cybersecurity Awareness: With the rising number of cyber threats targeting educational institutions, it's crucial for all users - students, faculty, and staff - to be aware of these threats and understand how to protect themselves and the institution.

2. Data Privacy and Protection: In an age where personal and sensitive data are constantly shared online, awareness of data privacy practices is vital. Educating the campus community about data protection helps safeguard personal information and institutional data.

3. Critical Thinking in the Digital World: Digital literacy also involves developing critical thinking skills to navigate the vast array of information available online, discerning credible sources, and understanding the implications of digital footprints.

Challenges in Implementing Digital Literacy Programs

Implementing effective digital literacy programs in educational institutions comes with its challenges:

- Diverse Skill Levels: The varying levels of pre-existing digital literacy skills among students, faculty, and staff make it challenging to design programs that are universally effective and engaging.

- Resource Allocation: Allocating sufficient resources, both in terms of funding and time, to develop and maintain these programs can be a hurdle, particularly for institutions with limited budgets.

- Keeping Pace with Technological Changes: The digital landscape is constantly evolving, and keeping educational programs up-to-date with the latest trends and threats can be daunting.

The Goals of Digital Awareness Programs

The primary goals of digital awareness programs in educational settings are to:

1. Equip Individuals with Essential Digital Skills: This includes basic technical skills, cybersecurity best practices, and an understanding of digital rights and responsibilities.

2. Promote Safe and Responsible Use of Technology: Encouraging behaviors that protect users and the institution from digital risks.

3. Foster a Culture of Lifelong Digital Learning: Cultivating an environment where continuous learning and adaptation to the digital world is valued and supported.

Developing Comprehensive Digital Literacy Programs

Integrating Digital Literacy into the Curriculum

A critical step in enhancing digital awareness is the integration of digital literacy into the educational curriculum. This integration ensures that students are not only exposed to the necessary technological skills but also understand the broader implications of digital technology in society.

1. Curriculum Design: Developing a curriculum that incorporates digital literacy should be a collaborative effort involving educators, IT professionals, and curriculum designers. The curriculum should cover key areas like online safety, digital ethics, information literacy, and basic cybersecurity principles.

2. Age-Appropriate Content: The digital literacy curriculum should be tailored to different educational levels, ensuring that content is age-appropriate and relevant. For younger students, the focus might be on online safety and etiquette, while older students could delve into more complex topics like data privacy and cybersecurity.

Professional Development for Educators

To effectively teach digital literacy, educators themselves need to be well-versed in digital technologies and cybersecurity. Ongoing professional development is essential in equipping educators with the necessary skills and knowledge.

1. Training Programs: Regular training programs should be established to keep educators abreast of the latest digital trends and threats. These programs can include workshops, online courses, and peer-learning sessions.

2. Resource Availability: Providing educators with access to resources and materials on digital literacy and cybersecurity can help them integrate these topics into their teaching more effectively.

Challenges in Curriculum Integration and Educator Training

- Resource Constraints: Developing a comprehensive digital literacy curriculum and providing ongoing educator training requires significant resources, which can be a challenge for some institutions.

- Engaging Content: Creating engaging and relevant digital literacy content that resonates with students can be challenging, particularly given the rapid pace of change in the digital world.

- Teacher Readiness: Ensuring that all teachers are prepared, and comfortable teaching digital literacy topics requires sustained commitment to professional development.

Leveraging Technology for Digital Literacy

Utilizing technology itself as a tool for teaching digital literacy can be highly effective. This can include the use of educational software, online platforms, and interactive tools that provide hands-on experience with digital technologies.

- Interactive Learning Tools: Incorporating interactive tools and simulations can make learning about digital literacy more engaging and effective.
- Online Platforms: Utilizing online platforms for teaching digital literacy allows for a more flexible and accessible learning experience, which can be particularly beneficial in remote or blended learning environments.

Cultivating a Cybersecurity Mindset Across Campus

Creating a Proactive Cybersecurity Culture

Cultivating a cybersecurity culture on campus involves more than just imparting knowledge; it's about developing a mindset where every member of the community actively contributes to the institution's digital safety. This cultural shift is crucial in creating an environment where cybersecurity is not seen as the sole responsibility of the IT department, but as a collective commitment shared by all.

Strategies for Building a Cybersecurity Culture

1. Regular Awareness Campaigns and Workshops: Organize ongoing campaigns and interactive workshops that address current cybersecurity threats and best practices. These should be engaging and relevant to the audience, using real-life scenarios and examples.
2. Promoting Cybersecurity as a Shared Responsibility: Encourage a sense of shared responsibility for cybersecurity. This can be done through communications that emphasize the role of each individual in protecting the institution's digital assets.
3. Creating Visible Cybersecurity Resources: Establish visible and easily accessible resources, such as online portals or help desks, where community members can find information, report concerns, and get support on cybersecurity matters.

Engaging Students in Cybersecurity Initiatives

Student involvement is a key component in fostering a campus-wide cybersecurity culture. Engaging students through clubs, competitions, and involvement in cybersecurity initiatives not only enhances their learning but also contributes to a more secure campus environment.

1. Cybersecurity Clubs and Societies: Support the formation of student-led cybersecurity clubs or societies. These can be platforms for peer learning, guest lectures, and practical exercises.

2. Participation in Cybersecurity Competitions: Encourage participation in national or international cybersecurity competitions, which can be highly motivating and provide practical, hands-on experience.

3. Project-Based Learning: Incorporate cybersecurity projects into relevant courses, allowing students to apply their theoretical knowledge in real-world scenarios.

Challenges in Fostering a Cybersecurity Culture

- Engagement of the Community: Keeping the entire campus community engaged and informed about cybersecurity can be challenging, especially in larger institutions with diverse populations.

- Balancing Information Overload: With the vast amount of information available on cybersecurity, it's important to strike a balance so that key messages are not lost in the noise.

- Resource Allocation: Allocating resources for regular campaigns, workshops, and student initiatives requires commitment and planning from the institution's leadership.

Measuring the Impact of Cybersecurity Culture Initiatives

Assessing the effectiveness of efforts to build a cybersecurity culture is crucial. This can be achieved through surveys, feedback after training sessions, and monitoring the number of cybersecurity incidents over time. Regular assessment helps in fine-tuning the approach and ensuring that the initiatives remain relevant and effective.

Summary of Section 2 Recommendations

Part I - Hardening Campus Information Security and Networks

1. Implement Advanced Cybersecurity Measures: Deploy firewalls and Intrusion Detection and Prevention Systems (IDS/IPS) to monitor and control network traffic. Regularly update software and manage patches to protect against vulnerabilities.

2. Enhance Network Security: Utilize network segmentation to isolate and contain threats. Secure Wi-Fi networks with the latest protocols and monitor for unauthorized access.

3. Data Encryption and Backup: Encrypt sensitive data both in transit and at rest. Implement a robust data backup strategy with regular testing to ensure data integrity.

Part II - Protecting Campus Critical Infrastructure

1. Conduct Regular Risk Assessments: Identify potential threats and vulnerabilities to both physical and digital assets. Regularly update and adapt risk mitigation strategies.
2. Develop and Implement Emergency Response Plans: Establish clear protocols for various types of emergencies, including cyber incidents. Ensure efficient communication channels and clearly defined roles.
3. Business Continuity and Disaster Recovery: Create and maintain plans to ensure the continuity of critical functions in the face of disruptions. Include backup systems and alternative operational procedures.

Part III - Enhancing Digital Awareness Programs

1. Integrate Digital Literacy into Curriculum: Develop age-appropriate digital literacy content and embed it in the educational curriculum across different levels.
2. Professional Development for Educators: Provide ongoing training and resources to educators on digital literacy and cybersecurity.
3. Create a Culture of Cybersecurity: Conduct regular awareness campaigns and workshops. Engage students through cybersecurity clubs, competitions, and project-based learning. Promote cybersecurity as a shared responsibility across the campus.

SECTION #3

Cybersecurity K-12 Education

Prepared By:

Dr. Chuck Gardner, Senior Advisor for Workforce Development, Cyber Innovation Center

Section Introduction

Education has been identified as a priority sector for the Cybersecurity and Infrastructure Security Agency (CISA). Entities that CISA Director Jen Easterly cite as "target-rich and resource-poor" [17] such as K-12 institutions, are hot targets for ransomware and other malicious attacks. "While schools are not considered critical infrastructure, they represent a soft target that is frequently hit by debilitating ransomware attacks." [18]This chapter will dive into the cybersecurity opportunities that primary, secondary, and post-secondary educators, facilitators, faculty, staff, and administrators can employ in classrooms or across campus facilities.

Section Overview

Conversations that occurred during this chapter development work included the topics of:

- K-6 Academic Support & Skill Development
- Cybersecurity 7-12 Career Technical Education
- STEM/STEAM
- Cybersecurity Professional Development Events
- Cybersecurity Competitions and CTFs
- ESports
- Digital Awareness/ Information Literacy, etc.
- K-12 Campus Infrastructure
- K-12 Access to Industry Recognized Professional Certifications
- Dual Enrollment

---

[17] Kapko, M. (2022, October 21). CISAs Priority Sectors for 2023: Water, Hospitals, K-12. Cybersecurity Dive. Retrieved on December 13, 2023, from https://www.cybersecuritydive.com/news/CISA-water-schools-healthcare/634657/

[18] Kapko, M. (2022, October 21). CISAs Priority Sectors for 2023: Water, Hospitals, K-12. Cybersecurity Dive. Retrieved on December 13, 2023, from https://www.cybersecuritydive.com/news/CISA-water-schools-healthcare/634657/

K-6 Academic Support & Skill Development

At the forefront of cybersecurity instruction lies the K-6 audience. Students at this age are either early language learners or early middle school-age students learning to engage with the communities that they live and play in. In order for these students to be engaged by resources that are developed for them, authors and content developers must take into account this wide disparity of learning modes – from the very graphical to the mid reader.

To that end, there are a variety of cybersecurity resources that are available to support academic and skill development of the K-6 population. Specifically, this section discussed contributions that are being made by CSTA (2023) and their K-12 Computer Science Standards, CYBER.ORG (2023) and their K-12 Cybersecurity Learning Standards, and NICE (2023) and their Cybersecurity Workforce Framework. Participants also realize the need to expand not only the capability of K-6 educators, but the quantity of those teachers. There are functional models available for other specialties including how JRTOC is supporting the development of computer science and cybersecurity instructors (CSforAll, 2023), how ISACA is working with regional chapters to train teachers on how to deliver cybersecurity and data science content in the classroom, and how the US Department of Education has support for teachers in the form of Digital Literacy Accelerators to bring partners from the community together to work to "create and pilot edtech innovations focused on digital literacy" (USDOE, 2023).

References:

Computer Science Teachers Association. (2023). K-12 Standards. Retrieved from https://csteachers.org/k12standards/

CSforAll. (2023). JROTC-CS Demonstration Project. Retrieved from https://www.csforall.org/projects_and_programs/jrotc/

CYBER.ORG. (2023). CYBER.ORG K12 Cybersecurity Learning Standards. Retrieved from https://cyber.org/standards

National Initiative for Cybersecurity Education. (2023). NICE Cybersecurity Workforce Framework. Retrieved from https://niccs.cisa.gov/workforce-development/nice-framework

US Department of Education. (2023). Digital Literacy Accelerator. Retrieved from https://tech.ed.gov/dla/

Cybersecurity 7-12 Career Technical Education

While most cybersecurity curriculum in the 7-12th grade arena typically falls within the area of Career Technical Education (CTE), there are examples of schools and districts that use the umbrella of computer science to house cybersecurity instruction. This topic explored a variety of educational and professional organizations that are working to provide exemplary models of

7-12 curriculum for use in the classroom. The Association for Career and Technical Education (ACTE) has a website dedicated to supporting teachers as they prepare students with career based education (2023); the National Security Agency (NSA) has a 114 page "CTE K12 Career Pathways for Cybersecurity" report that was published in late 2022 (2022); in 2020, CYBER.ORG published "The State of Cybersecurity Education in K-12 Schools" to help guide teachers, schools, and communities around what the ingredients are for a successful cybersecurity program (2020).

Additional research and examples from organizations that are working to monitor school access to cybersecurity resources and support teacher professional development include the work that Dark Enterprises has done to identify where students are being exposed to cybersecurity content in the high school classroom (2023). There are also a variety of state models that are expert at distributing and disseminating best practices in education including programs that operate in New York State and North Dakota.

In New York, there is a program called BOCES, or Boards of Cooperative Educational Services, that was a product of 1940's legislation that became such a cornerstone of educational support across the state that it was written into permanent law. One of the services that BOCES provides is to help unify curriculum offerings across the state by providing lists of approved curriculum and professional development providers. North Dakota's EduTech is a similar state-backed service that provides support and professional development for classroom teachers of all subjects, not just electives or CTE courses. The state of Arkansas employs a team of computer science specialists, or CSS, that work to ensure all districts and schools have the knowledge and support that they need to implement effective models of CS and cybersecurity instruction.

Microsoft TEALS (Technology Education and Literacy in Schools) is a philanthropic program supported by Microsoft. It is an initiative aimed at increasing access to computer science education in schools. TEALS pairs computer science professionals from the tech industry with classroom teachers to co-teach computer science courses. In 2021, TEALS partnered with CYBER.ORG to support the instruction of their Cybersecurity curriculum in classrooms across the country. At no cost to the host school, teachers can partner with Microsoft TEALS to identify industry professionals from the area to visit classrooms and directly support teacher instruction.

This section also discussed opportunities to increase the quantity of cybersecurity educators in the 7-12 space. More availability to quality professional development would be the easy win, but conversations also focused on more opportunities for teachers to earn credential training and testing from a variety of national and international credential organizations. It also discussed the opportunity for teachers to hold multiple credentials and the increased use of competitive platforms like Cyber Patriot to not only increase the ability of students but to also help train teachers. Lastly, the group discussed opportunities to provide increased awareness of ISC2's Center for Cyber Safety and Education's iamcybersafe.org page, in order to reach and inspire teachers and parents.

STEM/STEAM

STEM is science, technology, engineering, and math. STEAM is the integration of science, technology, engineering, arts, and mathematics, and can provide a multidisciplinary approach to cybersecurity education, making it more accessible and exciting for students. It encourages critical thinking, collaboration, and creativity while equipping them with essential skills for the digital age. There were two primary resources that were discussed that provided opportunities for teachers and students to blend art with STEM and cybersecurity instruction.

Code/Art is a non-profit organization that is based in Miami, FL, whose mission is to "increase the number of girls studying computer science by delighting and inspiring them with the creative possibilities of computer programming" (2023). They sponsor a number of girl-based programming competitions throughout the school year, such as "CodeYourSelf," "Coded Animated Art," "Game Design," and "ChangeMaker."

The Micro:bit Educational Foundation (2023) and CYBER.ORG have a number of STEAM-themed programming opportunities for students in K-12. CYBER.ORG's Coding Fundamentals curriculum (2023) works to implement cybersecurity into the platform by having students start with simple art and animation, but work towards projects that focus on conversations about cybersecurity. Using the micro:bit along with Microsoft's MakeCode editor, students can build a variety of encryption devices. Using the Python editor, students can begin to learn about advanced Python topics such as dictionaries and how to send encrypted messages, and then, using a variety of micro:bit devices, begin to understand wireless packets, denial of service and replay attacks, and even model a brute force attack demo in the classroom.

References:

Code/Art. (2023). Our Mission. Retrieved from https://www.code-art.com/about/

CYBER.ORG. (2023). Coding Fundamentals. Retrieved from https://cyber.org/coding-fundamentals

Micro:bit Educational Foundation. (2023). Create: Learn: Code. Retrieved from https://microbit.org/

Cybersecurity Professional Development Events

Professional development for K12 teachers is essential to ensure that they have the knowledge and skills necessary to effectively teach subject matter to students. In the area of cybersecurity instruction, effective professional development can lead to higher student engagement and increased awareness of cybersecurity issues among students. The conversations explored five of the widely regarded exemplar models for cybersecurity professional development in the United States.

The National Initiative for Cybersecurity Education (NICE) comes from the National Institute for Standards and Technology. Annually in December, NICE hosts their two-day K-12 Cybersecurity Education Conference (2023). The event brings together hundreds of K-12 educators from across the country alongside representatives from industry, academia, and the government, to provide opportunities for networking and collaboration. Breakout sessions, panel discussions, and the highly energetic "Cybersecurity Signing Day" event are just a few of the components of the conference.

Annually in June, CYBER.ORG hosts their EdCon for K-12 cybersecurity teachers from across the country. This two-and-a-half-day event includes breakout sessions and keynotes "designed to inspire and empower novice and expert K-12 cybersecurity educators and counselors alike" (2023).

TeachCyber's National Cybersecurity Teaching Academy "is a 12-18 credit hour graduate certificate for high school teachers. It includes coursework on teaching cybersecurity, foundations of cybersecurity, network security, and advanced topics" (2023). Offered in partnership with four universities from across the country, this virtual program provides expert, tailored instruction for experienced teachers who are teaching or want to teach cybersecurity.

Code.org offers a variety of professional development opportunities for new and experienced teachers. Their professional learning page offers options for elementary and middle/high school teachers (2023).

Project Lead the Way (PLTW) offers annual cybersecurity professional development for educators that will help them "develop the conceptual and instructional understanding you'll need to guide students as they learn about the ever-growing and far-reaching field of cybersecurity" (2023).

References:

Code.org. (2023). Professional Learning. Retrieved from https://code.org/educate/professional-learning

CYBER.ORG. (2023). CYBER.ORG EdCon. Retrieved from https://cyber.org/EdCon

National Institute for Standards and Technology. (2023). NICE K12 Cybersecurity Education Conference. Retrieved from https://www.nist.gov/itl/applied-cybersecurity/nice/events/nice-k12-cybersecurity-education-conference

PLTW. (2023). Professional Development for Teachers. Retrieved from https://www.pltw.org/professional-development/training-schedules

Teach Cyber. (2023). National Cybersecurity Teaching Academy. Retrieved from https://teachcyber.org/ncta-information/

Gamification: Cybersecurity Competitions, CTFs, and ESports

By incorporating game elements into the learning process, education can become more interactive, exciting, and relatable for students. Cybersecurity concepts are transformed into thrilling challenges, puzzles, or even virtual simulations where students can apply their knowledge in a practical and engaging way. Gamification can spark interest while promoting problem-solving skills, critical thinking, and teamwork, all while adding an element of competition to motivate students to continuously improve cybersecurity knowledge and skills.

Throughout the K-12 cybersecurity landscape, there are three exemplary cybersecurity competitions, two programming/ robotics competitions, and dozens and dozens of CTF, or Capture the Flag events that students can engage in. Within the realm of cybersecurity, the three competitions that most educators find useful are CyberPatriot (https://www.uscyberpatriot.org/, also known as the National Youth Cyber Education Program), sponsored by the Air and Space Forces Association, the National Cyber League (https://cyberskyline.com/events/ncl), sponsored by CyberSkyline, and CyberStart America (https://www.cyberstartamerica.org/), sponsored by SANS and the National Cyber Scholarship Foundation.

In the cybersecurity-connected world of computer programming and robotics, there are probably no bigger competitions than Vex (https://www.vexrobotics.com/competition) and Lego Robotics (https://www.firstlegoleague.org/). Each of these competitions engage students in every aspect of STEM while promoting all of the positive elements of gamification, including cooperation, critical thinking, and problem solving.

CTFs, or Capture the Flag competitions, are a convenient and typically virtual method of engaging students in the competitive nature of cybersecurity that lets them participate at various levels that help build confidence and content knowledge. There are many CTF events but be aware that some are not appropriate for K-12. As a result, NICE has compiled a K-12 cybersecurity competitions guide (2023) that can help teachers make sense of CTFs and even includes many of the competitions mentioned above.

References:

National Initiative for Cybersecurity Education. (2023). K12 Cybersecurity Competitions One-Pager. Retrieved from https://www.nist.gov/document/nice-k12-subgroup-competitions-one-pager

Digital Awareness and Information Literacy

The digital landscape is changing rapidly for our students. Cultivating digital awareness and information literacy skills among K-12 students is now more crucial than ever. They must have the skills to critically evaluate sources, discern fact from fiction, and navigate the complexities of the online world. However, it's not just about teaching them how to use technology; it's about

engaging in meaningful discussions that address the ethical, social, and emotional aspects of their digital lives. By integrating digital awareness and information literacy into the curriculum, leveraging interactive activities and real-life examples, and encouraging open dialogue, we can equip our students with the tools they need to navigate the digital landscape confidently.

The group's conversations found that there are many resources available for not only educators, but that can also enable caregivers, volunteers, and community members with the skills needed to host these conversations. Specifically, the Girl Scouts of the USA host two resources that are worth mentioning in this topic: their Cybersecurity Badges and the Cyber Awareness Challenge. Developed in 2018, the Girl Scouts Cybersecurity Badges "equip girls with the knowledge, skills, and hands-on experience necessary for them to thrive in the interconnected world we live in and to become the cybersecurity leaders of tomorrow" (2020). In a desire to promote both universal and equitable access to the concepts presented in the content, unplugged and low-tech badge activities are available at every level from Daisy (K-1) to Ambassador (11-12). The Cyber Awareness Challenge is an activities page hosted by the Girl Scouts that helps visitors (you don't need to be a Girl Scout to access this content) "learn about cybersecurity and how to protect yourself and others online" (2023).

In 2018, Palo Alto Networks developed the activity series that they call "Cyber A.C.E.S. – Activities in Cybersecurity Education for Students." The intent of the program was to enable Palo Alto Networks employees to volunteer in their community by delivering the content in the Cyber A.C.E.S. lessons to their residents. It's described as providing "the cybersecurity basics students need to have safer online experiences and become good digital citizens." (2023). The content is broken down into five age categories, including 5-7, 8-10, 11-13, and 14-15. Similar to the Cybersecurity Badges from the Girl Scouts, the content is primarily low- to no-tech and designed for ubiquitous access and equitable consumption. The materials are free to access but require an email to retrieve the download link.

CYBER.ORG has a number of free resources that help communities empower students and citizens with information on digital awareness and information literacy. Keys to Cybersecurity is one resource that provides a set of "self-paced, engaging activities designed to introduce students in 3rd - 8th grades to basic cybersecurity concepts" (2023). It requires no login and displays in any internet-connected browser, from cell phone or tablet to laptop or desktop. Two other initiatives from CYBER.ORG work to expand access to cybersecurity instruction across underrepresented and underserved populations.

Project REACH (Realizing Equitable Access to Cybersecurity in High school) and Project Access seek to support educators and students in regions that serve minority-serving higher education institutions and students with disabilities, respectively. Project REACH arms K-12 educators that have a feeder program to minority serving institutions (MSI) or historically black colleges and universities (HBCU) with cybersecurity resources and professional development. Project Access pairs subject matter experts with state agencies who are serving students who are low or no-vision, deaf or hard of hearing, or otherwise neurodivergent so that the agency can deliver

technical cybersecurity content to those students. Information about these two initiatives can be found at https://cyber.org/initiatives.

References:

CYBER.ORG. (2023). Keys to Cybersecurity. Retrieved from https://cyber.org/cyber-keys

Girl Scouts of the USA. (2020). Breaking the Firewall. Retrieved from https://www.girlscouts.org/includes/ceros/cyber-security/index.html

Girl Scouts of the USA. (2023). STEM: Navigating Cyberspace. Retrieved from https://www.girlscouts.org/en/activities-for-girls/for-every-girl/cyber-awareness.html

Palo Alto Networks. (2023). Cyber A.C.E.S. Retrieved from https://start.paloaltonetworks.com/cyber-aces.html

K-12 Campus Infrastructure

This chapter aimed to provide information relating to cybersecurity in K-12 facilities. While school security is not a principal focus of this overall section, it does warrant honorable mention, namely due to the fact that two organizations, CISA and the K12 Security Information eXchange (K12 SIX), have published guides that can support school administrators here.

CISA hosts their K-12 School Security Guide to "provide K-12 districts and campuses with resources, tools, and strategies to improve school physical security" (2023). CISA backs up their school security program mentioned above with an offer for a no-cost visit to any facility by a regional cybersecurity advisor (CSA) or physical security advisor (PSA). Broken up into ten regions across the country, CISA maintains a regional presence in every state, including the support of a large team of national CSAs and PSAs who perform local, on the ground review and analysis of facility defenses, all provided at no cost to the institution. The CISA Guide and Companion tools are required with no email registration. Facilities must contact their regional CISA office (https://www.cisa.gov/about/regions) to schedule a CSA/PSA visit.

Meanwhile, K12 SIX makes available their Essential Series, which "offers advice on pragmatic, actionable K-12 cybersecurity defenses - including a district self-assessment - and incident response resources" (2023). It also includes access to an annual report/ year in review document on the state of K-12 cybersecurity. All of these resources are free but require an email registration to access the download link for current publications. Archived publications are available without an email.

References:

CISA. (2023). K-12 School Security Guide Product Suite. Retrieved from https://www.cisa.gov/k-12-school-security-guide-product-suite

K12 SIX. (2023). The Report. Retrieved from https://www.k12six.org/the-report

K-12 Student Industry Recognized Professional Certifications

Career and technical education has supported the rapid evolution of K-12 education. Most notably, students enrolled in these programs now can graduate not only with a traditional diploma, but also with a variety of industry-recognized certifications. This shift equips students with practical skills and credentials that align directly with real-world industries and empowers them to enter the workforce with a competitive edge and clear pathway to their desired careers.

There are many content providers that are focusing some curriculum opportunities on industry-recognized certifications (IRC). Online learning partners include support from Udemy, Coursera, edX, and Pluralsight, to name a few. Teacher-delivered content partners include CYBER.ORG, the Virginia Cyber Range (US Cyber Range is an extension of the Virginia Cyber Range), Project Lead the Way, and others. There are YouTube publishers that have extensive resources to support student success on any number of cybersecurity credential topics, including those from Professor Messer and Certify Breakfast.

The group's discussions identified a number of certifying bodies that K-12 can expect limited amounts of success with, including CompTIA, ISACA, EC Council, Palo Alto Networks, Cisco, and ISC2, to name a few. While results do indeed vary from location to location, there are a few titles that have shown fairly high success rates when compared to others. In no particular order, those credentials where students are seeing success include CompTIA's ITF+ and A+ (Sec+ and Net+ are additional topics being presented in high school, but might not be as successful as ITF+ and A+), ISACA's Cybersecurity Fundamentals certificate and Information Technology Certified Associate (ITCA), the EC Council's Certified Ethical Hacker (CEH), Palo Alto Networks' Certified Cybersecurity Entry-level Technician (PCCET), Cisco's Certified Support Technician (CCST) and Certified Network Associate (CCNA), and ISC2's Certified in Cybersecurity (CC). While not an exhaustive list, these industry recognized credentials serve as valuable benchmarks for high school students, offering them the opportunity to demonstrate their proficiency in the field of cybersecurity, regardless of their current level of expertise.

Dual Enrollment

Dual enrollment refers to the practice of allowing high school students to participate in college-level courses, either at a local community college or on campus at a four-year institution. In the context of K-12 education, dual enrollment programs provide students with an opportunity to earn both high school and college credit simultaneously.

High schools that have higher education partners that offer dual enrollment courses can many times provide a relief valve for that high school needing to find a qualified (and in many cases, certified) cybersecurity teacher. Additionally, higher education institutions demonstrate their willingness to support K-12 instruction by offering dual enrollment programs because they typically serve two important goals for the institution: firstly, they provide an opportunity to engage high school students who may not have initially considered attending the college or university after graduation, effectively bringing them onto their campus or involving them in

their programs. Secondly, these programs enable the institution to award participating students with credit that can be applied towards earning a degree, thereby fostering a seamless transition from high school to higher education.

K-12 Education Recommendations

Many topics have been discussed in this chapter, from early language learners all the way through high school students earning industry recognized credentials and college credit. The recommendations will be broken into bullets, in an order that represents the topics as they've been presented throughout the chapter.

K-6 Academic Support & Skill Development, and Cybersecurity 7-12 Career Technical Education

- More teachers are needed to increase the capability of K-12 as a whole.
    - Math and science teachers can be tapped as leaders to bring cybersecurity into classrooms.
    - University programs that are teaching new teachers can support.
    - Partner with universities teaching cybersecurity – partners can be a force multiplier because content in most cases might be self-directed and hosted online.
    - Carrot vs Stick
        - Teachers are already overwhelmed. Schools should provide incentives for teachers to embrace cybersecurity curriculum.
    - States can develop teacher certification programs that are tailored to specific instructional levels.
        - How to teach cybersecurity to early learners vs advanced learners.
        - How to incorporate scenarios or labs into classroom instruction.
        - Employ a train the trainers or teach the teachers program to create peer-led instruction across districts.
    - Provide more opportunities and incentives for teachers to study/earn credentials.
        - Encourage districts to identify and retain multi-credential holders.

STEM/STEAM

- Schools and districts must identify methods to increase student diversity.
    - Inclusion of all learners, not just the math and science population.

- Neurodiversity is a must.
    - CISA has a DEIA goal that includes the cultivation of an inclusive culture that champions dignity, respect, and belonging where diverse talent is leveraged equitably to advance cyber and infrastructure security.

Cybersecurity Professional Development Events

- Recognizing that all teachers are at or near 100% of their teaching capacity, schools and districts must support these maxed-out teachers while investigating opportunities to expand coverage of cybersecurity across all grades and subjects.
    - Opportunities for cybersecurity education (both technical and non-technical) across all grades and subjects will ultimately relieve teachers in the long term because it will become a shared responsibility that can impact students at any point in their academic career.

Gamification: Cybersecurity Competitions, CTFs, and ESports

- This is an ideal space to reach students who have a goal or vision for engineering.
- Gamification of content has the ability to meet most students where they live, eat, work, and play
- Schools should look to include other competitive subject areas here, such as mathleats, science bowls, and computer science teams.
- Competitive arenas where students are rewarded for research and out-of-the-box thinking could also be an area where foreign language learners can find substantial success.
- There are many college and professional scholarships available for students who succeed in gamified events including CTFs and Esports.

Digital Awareness and Information Literacy

- Cyber hygiene must be a topic that is discussed at every level of society.
    - Schools and districts should be encouraging community members to follow up on the classroom conversations by supplying some of the academic resources for consumption by teams, volunteers, and general public audiences.
- Create more methods to increase student diversity.
    - In underserved areas, it may be challenging to support an increase in teacher responsibilities.
    - Opportunities for public and private industry contributions to classroom support and instruction should be investigated.

- Industry should be encouraged to incentivize their professionals to give back to the schools.

K-12 Campus Infrastructure

- Schools/districts should investigate opportunities to utilize CISA & K12 SIX resources.

K-12 Student Industry Recognized Professional Certifications

- In many cases, IRCs are neither cheap or easy.
  - Schools must realize that not all students are destined for success on IRC exams.
  - Teachers must be effective classroom leaders or facilitators to prepare students adequately for these exams.
  - Students will benefit in multiple ways from exposure to these exams:
    - They will gain an appreciation for the rigor of IRC tests.
    - If properly structured, failure (if it happens) can serve to strengthen a student's resolve to succeed in not only their everyday academics, but also to succeed in the industry.

Dual Enrollment

- K-12 schools should seek out higher education institutions with established cybersecurity programs to investigate the opportunities for dual enrollment credit.
- K-12 and Higher Education Institutions should work closely to develop foundational and introductory courses for dual enrollment purposes in U.S. high schools to community colleges to maximize the speed and efficiency of cybersecurity education preparation.
- Local school districts should work with all 9-12TH grade (high schools) and community colleges to design and utilize dual enrollment templates to assist in the rolling out of these programs across the country.

SECTION #4

The Traditional (Academic) Pathway Model- Cybersecurity Higher Education/Training Programs, Degrees, Certificates, Curriculum, and Standards-

Prepared By

Dr. Ulku Clark, Director of Center for Cyber Defense Education, University of North Carolina, Wilmington

Dr. Abdallah Haddad, Chief Information and Technology Officer, Lander University, SC

Joe Gibson, Information Security Officer, Trident Technical College, SC

Dr. Keith Clement, California State University, Fresno

Section 4 Overview

Section 4 starts with an introduction to reiterate the rising challenges of the cybersecurity workforce gap and the importance to bridge this gap and address the increasingly sophisticated cybersecurity threats and cybercriminal activities. Then, the section discusses the critical role that higher education plays in bridging the cybersecurity workforce gap, while presenting several strategies as well as recommendations that may be vital for higher education to not only serves as a hub to nurture cybersecurity skills, but also as a pipeline and a pathway for K-12 and college students to achieve sound and valuable professional or research careers in the cybersecurity field. Finally, the section concludes with a summary emphasizing the key role that higher education can play in bridging the workforce gap while implementing collaborative approaches and strategies with the support of private industries as well as government agencies to produce a well-prepared and qualified cybersecurity workforce.

Introduction

There is a consensus among industry, business, and cybersecurity leaders that cyberthreats and attacks have drastically increased and grown to highly sophisticated levels in recent years, forming a large, well-organized, and independent criminal economy. This new cybercrime ecosystem now includes cybercriminal packages and out-of-the-box services to novice and enthusiastic cybercriminals. Such offerings include easily deployable ransomware kits, malware packages, and access brokers. [1] [2] According to Cybersecurity Ventures, the cost of cybercrime is predicted to reach 10.5 trillion dollars annually by 2025; while Gartner analysts forecast that 45% of global organizations will be impacted by cybercriminal attacks. [1] [2] [3] In addition, a report by Cybersecurity Ventures indicated that the global ransomware market was valued at $20 billion in 2022 and is expected to grow to $265 billion by 2031.

The growing and alarming cybercriminal threats to world economies and safety are prompting leaders to take immediate, swift, and effective actions to combat these threats. One of these

actions or strategies is to ensure that there exists a very well-prepared, capable, and skilled cybersecurity workforce through which cyberattacks are thwarted and well-defended to minimize their costly impacts. Unfortunately, and as stated early in this paper, there currently exists a big gap in the cybersecurity workforce, prompting major concerns among industry, business, and government leaders. A report by the International Information System Security Certification Consortium (ISC2) showed that while the cybersecurity workforce has grown by 8.7% in 2022-2023, the gap between the number of cybersecurity professionals needed and the number of available positions has also grown at a rate of 12.6% (increase year over year). The report further indicated that the 2023 global cybersecurity workforce gap was at 3,999,964, with 482,985 vacancies in the United States alone (an increase of 17.6% from the year before). [4]

References/Footnotes

[1]https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf)

[2]https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf

[3]https://www.forbes.com/sites/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/?sh=4df761ff3b0c)

[4] *https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e*

The key Role of Higher Education: A Critical Pipeline for a Capable Cybersecurity Workforce

Higher education institutions can play a very critical and productive role in closing the cybersecurity workforce gap. Higher education institutions can serve as a hub for the development and production of a well-educated and capable cybersecurity workforce that not only encompasses specialized cybersecurity fields and curriculums, but also other disciplines and programs across all higher education curriculums (e.g., business, sciences, humanities, social sciences, engineering, and other disciplines). Such a workforce would be composed of those individuals who would possess expertise and high skills that are highly focused on cybersecurity and those individuals who would possess cybersecurity skills as an essential ingredient in their knowledgebase to achieve professional duties effectively and securely in digital societies and economies.

To ensure a robust cybersecurity pathway and pipeline, higher education can employ several strategies within its own ecosystem and in collaboration with K-12 school systems and other colleges as well as with industry and private sectors and government agencies. In addition, universities can transform the content of their curriculum to embrace cybersecurity as a specialized field or as a core topic within other fields as well as extracurricular collaborative

initiatives. The following paragraphs will address these strategies with accompanied recommendations for higher education to help bridge the cybersecurity workforce gap.

Collaborating with K-12 School Systems: Rich, Diverse, and Productive Pathway

The STEM (Science Technology, Engineering, and Mathematics) program serves as a great vehicle to equip secondary education students with the appropriate cybersecurity skills and abilities as they make their way to post-secondary education. Higher education institutions can play a very positive and productive role in strengthening such programs to facilitate and nurture the cybersecurity workforce pathway and pipeline. The STEM program starts in elementary schools; students are positioned to be equipped with comprehensive science skills and, to an extent, appropriate cybersecurity skills while being exposed to real-life cyber threat exercises and solutions. 5 Nonetheless, STEM should not be the only vehicle to ensure cybersecurity pathways; there should be programs and initiatives with wider scopes and more depth to promote and cultivate cybersecurity programs across K-12 schools and other platforms at the local, state, and federal levels. These educational programs can help bridge the gap between STEM and non-STEM disciplines by providing critical cybersecurity skills, awareness, knowledge, and abilities to all students across K-12, especially starting at the elementary levels. Skills and topics would range from basic digital literacy and cyber hygiene to coding and hands-on experiences as well as on cybersecurity careers.

These productive programs can and should be collaborated with higher education institutions and bridge programs as well as supported by private, local, state, and government agencies. For example, in 2023, York College collaborated with AT&T, under the NASA STEM program, to provide Queens students with foundational and critical cybersecurity skills through curriculum, research, and student-created projects. Students learned about the importance of cybersecurity careers to industries and economy, given the challenges of the cybersecurity workforce gap and how essential cybersecurity is to everyday digital life.8

In addition, such programs can also bridge the minority gap to ensure equal opportunities are available to cybersecurity careers and fields. For example, the “Partnership to provide technology and cyber-security experiences to Alabama Black Belt through mobile application development” Project is the product of the collaborative and partnership efforts between Auburn University, a rural and an urban school district in the historic Black Belt region of the state of Alabama, and Tuskegee University Engineering and Computer Science Alumni Associations. The project is aimed to engage students in cybersecurity hands-on experiences and laboratory-based tasks as well as mentorship experiences in the fields of computer science. The project is jointly co-funded by the Innovative Technology Experiences for Students and Teachers (ITEST) program and by the Established Program to Stimulate Competitive Research (EPSCoR), which receives funding from the National Science Foundation (NSF). 9

Government funding and private support should continue and strengthen these kinds of programs and initiatives to encourage additional partnerships and collaborative efforts with the private sectors and industry to develop a comprehensive approach to a well-prepared, well-

equipped, and diverse cybersecurity workforce capable of promptly addressing real-world challenges with creative solutions.

Moreover, these productive and critical programs and collaborative efforts, led by higher education institutions, should ensure that the cybersecurity curriculum and functions are in alignment with the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program, which is "managed by NSA's National Cryptologic School. Federal partners include the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Institute of Standards and Technology (NIST)/National Initiative on Cybersecurity Education (NICE), the National Science Foundation (NSF), the Department of Defense Office of the Chief Information Officer (DoD-CIO), and U.S. Cyber Command (USCYBERCOM). The NCAE-C program aims to create and manage a collaborative cybersecurity educational program with community colleges, colleges, and universities." 8

References

[5]https://irp.fas.org/eprint/cnci.pdf

[6]https://www.asisonline.org/security-management-magazine/latest-news/online-exclusives/2022/how-educational-institutions-can-help-fill-the-cybersecurity-workforce-gap/

[7]https://stelar.edc.org/poster/partnership-provide-technology-and-cyber-security-experiences-alabama-black-belt-through.

[8] https://www.york.cuny.edu/news/2021/nasa-maa-program-motivates-stem-students-

[9] https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

Partnerships among Universities and Other Agencies

Higher education institutions can collaborate with other colleges and universities under the sponsorships of government agencies and/or private organizations to equip and provide students with robust cybersecurity skills and pathways in alignment with established frameworks and standards such as NCAE-C and NICE. For example, The National STEM Consortium's (NSC) Cyber Technology Pathway is a one-year hybrid program (mixture of online and face-to-face) consisting of 12 mini-courses. It is one of five-certificate programs developed by the National STEM Consortium (NSC), with the collaborative efforts of ten colleges in nine states and funded by a grant from the U.S. Department of Labor. It offers participating students a cybertechnology certificate of 30 credits with learning outcomes mapped to the National Cybersecurity Workforce Framework, which is completed in collaboration with the Open Professional Education Network Platform+ program. Students are prepared and equipped to fill entry-level cybersecurity positions across industry and government agencies. Students also have an opportunity to sit for nationally recognized certifications from Cisco and CompTIA. 10

Another example that demonstrates the collaboration between colleges and other agencies is the partnership between the Naval Information Warfare Systems Command and the San Diego Community College District, which allows the offering of internship programs for college students, providing solid cybersecurity pathways. Students who become Naval Information Warfare Systems employees become eligible for subsidized education benefits. Students are hired for positions with a salary of up to $43,000 annually while they attend college. Those who earn bachelor's degrees can make initial annual salaries of more than $73,000 with the potential to increase to more than $125,000 annually. 11

Most importantly, the U.S. National Science Foundation (NSF) CyberCorps® Scholarship for Service program renewed its funding for seven academic institutions in 2023 through 2027. The funding included more than $24 million, which was added to prior investment of $29 million, throughout the funding period. This program funding supports the strong developments of a qualified and robust cybersecurity workforce that can address the recruitment and retention challenges of cybersecurity professionals to serve local, state, and government agencies. The awardees are part of 98 institutions participating in the CyberCorps SFS program across 39 states as well as the District of Columbia and the commonwealth of Puerto Rico, which demonstrate the investment in a diverse population. This population includes geographic and racial demographics such as historically Black colleges and universities as well as Establish Program to Stimulate Competitive Research (EPSCoR) universities. Almost all students who participated in these awarded programs were placed in federal cybersecurity positions, strengthening the cybersecurity workforce pipelines. These projects strongly support the practical education, development, and recruitment of greatly needed cybersecurity qualified professionals to face and address the rising challenges in this digital age. 12

There are similar other programs and efforts across the nation that lead to similar outcomes and should be supported and enhanced by private and government agencies. Higher education institutions should continue to augment the partnership and collaborative efforts with industry and government partners to effectively address and bridge the cybersecurity workforce gap with highly qualified cybersecurity professionals. Furthermore, higher education institutions can nurture and implement internships, apprenticeship programs, co-op programs, and practical projects with industry leaders and partners, sponsored and encouraged by government agencies such as NICE and NSF. The practical projects provide students with real-world situations and cybersecurity challenges while enhancing their skills and making them more valuable to rapidly fill cybersecurity positions. Plus, cybersecurity experts can provide insights and support regarding the latest cyberthreat trends, combating tools, and effective practices, making sure students are well prepared for real-world challenges and threats. In addition, higher education institutions are uniquely positioned to promote diversity and inclusion when bridging the cybersecurity workforce gap; they can include outreach programs and initiatives targeting underrepresented populations and attracting diverse students to pursue careers in cybersecurity.

References

[10] https://oli.cmu.edu/courses/cyber-technology-nsc-stem-pathways/

[11]https://www.cccco.edu/About-Us/News-and-Media/ccc-outlook-newsletter-archive/SDCC-Cybersecurity-Pathways

[12] https://new.nsf.gov/news/nsf-renews-cybersecurity-workforce-development

Higher Education Curriculums and Certifications

Higher education institutions can innovatively and creatively redesign their curriculums to be cybersecurity friendly supported by key relevant courses and experiential learning activities as well as certifications. There is evidence that certifications are necessary for graduating students to complement the cybersecurity curriculums in higher education, showing that one has demonstrated commitment to understand and succeed in cybersecurity professions. According to Fortinet report, reflecting the findings from a survey of 1,855 IT and cybersecurity decision-makers which was conducted by Sapio Research in November of 2022, most leaders greatly valued the specialized technical knowledge and skills of future or sought employees. Eighty-two percent (82%) of the respondents indicated that their organizations or companies would benefit from employees with cybersecurity certifications, and 90% indicated they would financially support employees to attain cybersecurity certifications. 13

In their research regarding the integration of certifications into college cybersecurity curriculums, Tran et al. (2023) found that Atlanta Georgia businesses, who hired cybersecurity recruits and interns, interviewed those with desired certifications, along with a college degree, when seeking potential employees for job placements in cybersecurity positions. 14 Furthermore, Tran et al.'s (2023) findings indicated that 94% of cybersecurity professionals were convinced that their certifications helped them obtain employment and successfully protect their organizations thereafter. Therefore, attaining cybersecurity certifications would add a substantial value to the students' cybersecurity toolbox along with a college degree, positioning the student to be well-equipped and prepared to enter the cybersecurity workforce.

Moreover, Tran et al. (2023) encouraged educators to be innovative in the delivery of instruction to include experiential learning and industry certifications. They also indicated that it was very critical for educators to stay abreast and informed regarding global cyber-attacks and threats to further educate and help their students learn relevant and modern cybersecurity skills and knowledge to effectively address and secure contemporary and digital workplaces. The faculty knowledge on the latest cybersecurity threats, the practical skills gained by students, and the enhancements of student outcomes with certifications allow university curriculums to stay relevant and current within the dynamic and ever-changing cybersecurity domain. This will help produce a stronger cybersecurity pipeline and pathway with a qualified workforce that is ready to fill vacant positions and meet industry and government needs.

Higher education institutions should closely work with industry leaders to incorporate certifications as part of their curriculums and capstone projects to ensure that graduates are fully equipped and prepared as they enter the cybersecurity workforce. By the same token, higher education institutions should be supported and funded via grants and private funding to encourage such directions; while students should be enticed with federal funding (e.g., financial aid) and scholarships to encourage efforts to obtain industry-recognized certifications as they obtain their higher education degrees.

Additionally, higher education institutions can develop focused cybersecurity curriculums that cover trends and topics in cybersecurity such as network security, social engineering trends, cryptography, ransomware trends, ethical hacking scenarios, mobile security, and incident response plans. Plus, cybersecurity projects and research can be implemented across disciplines with the collaboration and active involvement of faculty and students, enabling a holistic approach and understanding of cybersecurity threats and solutions. These curricular programs equip students with the required cybersecurity knowledge and skills to join the cybersecurity workforce promptly and effectively.

Higher education institutions should also be incentivized and encouraged by state and federal agencies to innovatively integrate established and industry-recognized certifications and training programs into their curriculums. Certifications such as CompTIA Security+, ISC2 Certified Information Systems Security Professional (CISSP), Offensive Security Certified Professional (OSCP), or Certified Ethical Hacker (CEH) not only add value to students' academic credentials but ensure that students conduct hands-on project and experiential learning activities to seamlessly transition into the cybersecurity workforce.

References

[13] https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf

[14] Tran, B., Benson, K. C., & Jonassen, L. (2023). Integrating certifications into the cybersecurity college curriculum: The efficacy of education with certifications to increase the cybersecurity workforce. Journal of Cybersecurity Education, Research and Practice, 2023(2), 2.

Cybersecurity Training and Awareness Among Students and the Community

There are indications that most K-12 and college students lack the necessary cybersecurity knowledge and skills to protect their data and their computing devices while using the Internet and digital resources in this critical digital age. For example, according to cyber.org, the results of a nationally representative survey that was administered by the EdWeek Research Center in 2020 of more than 900 K-12 teachers, principals, and district leaders, suggested that students as well as educators had limited knowledge and skills of cybersecurity and internet safety. Plus, less than half of the respondents reported that their districts or schools offered cybersecurity education. The survey presented twenty-one (21) questions about cybersecurity education that

pertained to students' understanding of how their connected electronic devices interacted with the Internet, how to protect their digital assets from vulnerabilities, and moral and ethical issues surrounding the uses of technology.

The survey result showed that the majority (91%) of respondents did not know "a lot" about cybersecurity education in public schools (51% knew some, 29% knew a little, and 10% knew none). But more disturbing was that educators reported that their students knew less than they did about cybersecurity. Furthermore, the results showed that access to cybersecurity education is infrequent and unequal, while access to cybersecurity education resources was not consistent across communities and education settings with private schools showing higher access to cybersecurity education. The results suggested that more privileged students had better opportunities to be exposed to the cybersecurity field. The lack of access to these resources in public schools may lead to lack of interest in cybersecurity careers. In addition, most cybersecurity education in K-12 are based on standards and rubrics set by the department of education in each relevant state, such standards are infused into the curriculum program within mainly the science areas such as computer science. 15

References

[15] https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf

Unfortunately, this lack of basic cybersecurity awareness and education spills over to higher education as there are no core, general, or extracurricular courses or training that would equip students with essential knowledge and understanding of cybersecurity threats and how to protect their data and university data. While there is a little or no studies in the U.S. to gauge college students' knowledge, understanding, and readiness to protect data or devices against cyberthreats as they use online resources, one only needs to read news and hears of incidents and comprised credentials because of phishing emails and unprotected computers. Most students are unbale to identify cyberthreats and fall as victims while giving their credentials and sensitive information to cybercriminals. An older research survey conducted in two California State Universities in Silicon Valley in 2017-2018 showed that despite the technical knowledge of students and their belief that they were tracked and observed when using the Internet and that their data was not secure, students were still not aware of how to protect their data. 16 In addition, some studies conducted outside the U.S. presented serious concerns regarding the lack of cybersecurity knowledge and awareness among college students

Post secondary education can play critical roles in collaborating with and helping K-12 students and educators as well as their own community by offering both essential cybersecurity training session and activities regularly and on annual basis as well as core cybersecurity modules that could be built into freshman success seminars and classes and lifelong learning programs. Essential cybersecurity training sessions could align with the national cybersecurity awareness month of October. Furthermore, K-12 and post-secondary institutions can collaborate with or leverage the plethora of resources made available by the Cybersecurity and Infrastructure

Security Agency (CISA), which is the highest government agency for national risk management and cyber and physical infrastructure. CISA offers a wide range of cybersecurity and training resources, including K-12 and college level programs and training courses. These training activities can be designed to align with extended CIS frameworks and established guidelines based on current challenges and solutions. Such programs should be supported and sponsored by private and government agencies. Moreover, colleges should encourage the formation of cybersecurity clubs or student organizations where participants would engage in cybersecurity workshop activities, competition events, and collaborative projects. These extracurricular activities promote and cultivate cooperative learning activities, networking exercises, and practical skill developments among the participants.

In collaboration with K-12, community leaders, and industry leaders, post-secondary education should organize seminars, webinars, and presentations to include industry cybersecurity experts and experienced professionals as well as researchers. These events would include emerging trends, case studies, career pathways, and best practices in cybersecurity. Additionally, higher education institutions should ensure students have access to cybersecurity resources including online tutorials, books, journals, and subscription-based resources and organizations with discounted or free access to relevant tools and software.

Furthermore, post-secondary education should arrange and encourage students to participate in cybersecurity competitions such as hackathons, capture the flags, and cyber defense; these hands-on events simulate practical scenarios, foster problem-solving skill development, teamwork collaboration, and technical proficiency. Collaborating with other colleges and private agencies, higher education institutions can offer and facilitate cybersecurity career counseling services and mentoring programs, pairing students with mentors who are experienced cybersecurity professionals and who can provide advice, guidance, and cybersecurity insights and careers.

References

[16] Moallem, A. (2019). Cyber security awareness among college students. In *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA 9* (pp. 79-87). Springer International Publishing.

https://scholarworks.sjsu.edu/indust_syst_eng_pub/30/

National Cybersecurity Career Education Pipelines and Pathways Framework

It should be noted that the K-12 Education Community is a key partner and major stakeholder on the front-end of a career pipeline and pathway as higher education relies on the outputs of K-12/Adult Education Systems. In addition, higher education must include a variety of critical industry based certification programs for their degree programs to fully meet most cybersecurity position minimum requirements (like CompTIA Security+ for example). In addition cyber education pipeline/pathways must have “On the Job” Training components as well.

Cybersecurity job seekers with less than a minimum of 1+ year of increasing IT/Security responsibilities/positions will find it very difficult to break into the field here with only a degree and smattering of professional certifications.

Cybersecurity career education pipelines and pathways are made up the following components.

K-12 Education Connection and Link (see Report Section 3)

Dual Enrollment- K-12 & CC count them as enrolled students- a more efficient pathway

Adult Education Systems

2- Year Community College Programs (Degrees, Certificates)

4- Year University Undergraduate Programs (Degree, Certificates)

6- Year Graduate Degree Programs (Degree, Certificates)

Doctoral Programs and Post-Doc Opportunities

IT-Cybersecurity Academies & Bootcamps

Industry Recognized Professional Certifications (Section 7)

Workforce Development and the On the Job Training (like apprenticeships) (Section 8)

Additional Caveats:

1. All cyber degree programs must balance and include the academic disciplines of: computer science, business, electrical/computer engineering, and social sciences/liberal arts.
2. Map and stack certifications into degree programs; students are also earning "Credit for Prior Learning"; fusion of professional and academic credit (see Report Section 7).
3. Integrate certifications into higher education academics; (see Report Section 7).
4. Different ways of linking certs into higher education; see Report Section 7).

Programs – Mostly Recommendations, Some Context

Associate, Bachelor, and Graduate Cybersecurity degree and certificate programs should endeavor to meet the National Centers of Academic Excellence in Cybersecurity (CAE-C) program criteria jointly sponsored by the National Security Agency (NSA) and the Department of Homeland Security (DHS). Degree curriculum and workforce training programs must be based on common frameworks and standards like the NIST Cybersecurity Framework and CIS

Critical Security Controls. Cybersecurity degree and training programs must be flexible to respond to the continually evolving threat environment and safeguards landscape. Effective programs include hands-on labs and real-world projects to provide students with practical experience. Moreover, programs would involve simulations, virtual environments, and cybersecurity competitions. Programs must embrace a coordinated and balanced multidisciplinary approach that includes computer science, business, electrical/computer engineering, and social sciences/liberal arts.

Programs (Intern/Apprentice)

Strengthening program offerings through industry partnerships must also be a key focus. Curriculum change processes should be inherently agile to maintain relevance and value. Programs should emphasize continuous learning and adaptability to prepare students for ongoing changes in the cyber threat and defense ecosystem. Furthermore, programs that offer internship support, job placement services, and connections with industry partners help students transition into the workforce more smoothly.

Apprenticeship opportunities help dual enrollment high school and college students gain experience and form relationships with employers that lead to full time employment.

Cyber Instructor

Cybersecurity instructors with practical experience and in demand cybersecurity certifications provide valuable insights to students. These instructors can also impart critical knowledge and advocate for industry certifications.

Student Certifications.

Students should be required to complete certification exams soon after completing cybersecurity courses that specifically prepare for certification.

Cyber competitions, clubs, bootcamps

Cyber competitions create interest in cybersecurity degree and training programs with K-12 and higher education students. Cybersecurity clubs also serve as a motivating factor to get involved in the cybersecurity field.

Cybersecurity bootcamps provide baseline skill up training that strengthen small and midsize businesses and complement 3rd party managed services.

Digital Awareness and Information Literacy

As we ponder the “big picture” as well as the public and academia “categories,” “Information Literacy” comes to mind. Given the value of information/data across all sectors of our societies, it would seem natural that the topic of Information Literacy would need to be infused into curriculums at all levels (K-12 - post secondary). Just like literacy about the value of “money”

and "currencies" is/are being infused into the curriculums, Information Literacy may also need to be infused not only to create awareness of how critical information security is, but also to create appreciation, understanding, and interest of the information security field at early ages and build on it thereafter while naturally and seamlessly enhancing the national cybersecurity education and workforce development. This work is very important, especially at a critical juncture of the Information Age.

Cybersecurity Higher Education Components

We must include and balance the following components into a comprehensive strategy for implementation to enhance cybersecurity education and higher education utilizing a career pipeline/pathway approach. We have spoken about the K-12 side already (i.e. see Section 3); and now we discuss higher education (academic) degrees and certificate programs;

1. Academic Programs, Courses, Curriculum and Standards-
2. Professional Industry Recognized Certifications- demonstratable skills needed by employers—showing competencies, etc.
3. Professional Development- group projects in coordination/partnership with industry and employers; help students into the career path through leadership and mentoring.
4. Workforce Experience- Critical! Even volunteer stuff!
5. Cyber Competitions- CTF stuff—students that work on their own in CTFs are the kinds of employees that we want in our cybersec firms.
6. Campus cyber awareness, training, and exercises.

What we need in this area:

Value of superior communications skills- oral, written, high emotional IQ

Technical versus non-technical positions-

Must understand business and the process driving the business-

Understand basic technology and security professionals-

Cybersecurity Workforce Development Multiple Pathways Models:

1. Higher Education Pathway- 4-year/ 6-year degrees and certificates
2. Workforce driven Pathway- Flip the model—apprenticeship driven; education and training not found on the college/university campus.
3. Auto-didactic learners- self-taught cybersecurity preparation (for example: hackers)

We must braid the following into cyber education/training:

1. Education/training programs
2. Industry recognized professional certifications
3. Workforce Opportunities- apprenticeship, internship, co-op

Table 3: Cybersecurity Carer Education Pipeline-Pathway Components

Soft Start Cybersecurity Programs- start slow and bring learners up to speed-

K-12- College Readiness and Career Preparedness

- Academics and skill building- 3RD grade math/english @ level
- Science, Technology, Engineering, Math (STEM)/STEAM
- 7th grade- Career Technical Education (CTE)
- Cyber Hygiene (All Levels of Education)
- Dual Enrollment

Higher Education

2-Year Degrees/Programs

4-Year Degrees/Programs

6-Year Degrees/Programs

Ph.D. Programs

Academic Stacking Certifications & Industry Recognized Professional Certifications-

Workforce and Professional Development Experience-

Section 4 Conclusion

Undoubtedly, higher education institutions can play critical important roles serving as a hub and gateway to help bridge the cybersecurity workforce gap. It is critical that information literacy would need to be infused into curriculums and extra curriculums at all levels in K-12 and post-secondary education. Just like literacy about the value of “money” and “currency” is being infused into the curriculums in K-12 and in freshmen success seminars in postsecondary education, information and digital literacy, focusing on cybersecurity, must also be infused into the higher education curriculums not only to create awareness about the importance to protect data, but also to create appreciation, understanding, and interest in information security throughout the student learning cycle. Such constant learning blocks can serve as pillars to continuously build on while naturally and seamlessly enhancing national cybersecurity education and workforce development.

This diligent and coordinated work is very important, given the widening cybersecurity workforce gap, especially at our current critical juncture of digital economies that are facing colossal cybersecurity threats. Higher educational institutions should build seamless bridges between K-12, community colleges, private industry, renowned security organizations, and government agencies to ensure curriculums, activities, collaborative and partnership programs, certifications, and assistantships are promoted and supported in alignment with the industry cybersecurity needs and gaps as well as security frameworks and standards (e.g., NCAE-C and NICE). With meaningful and incentivized funding and support by government agencies and private organizations, higher education institutions can play highly productive role in filling the growing cybersecurity workforce gap and effectively combat the increasing cybercriminal threats and online criminal activities.

SECTION #5

The Non-Traditional (Experiential) Pathway Model- Building and Enhancing U.S. Cybersecurity Education and Workforce Development Infrastructure, Capabilities, & Capacity Through Professional Development, Pre-Apprenticeships, Registered Apprenticeships

Prepared by

Dr. Keith Clement, California State University, Fresno

Section 5 Overview

Report Section 5 introduces and describes the value and importance of developing/implementing cybersecurity career education non-traditional pathways.

Identify "non-traditional" cybersecurity career education pathway and component parts.

Alignment and linkages with IT-Cybersecurity professional development opportunities like Cyber Academies, Bootcamps, Cyber-competitions, hackathons, and related events and activities.

Alignment and linkages with education/training programs and Industry Based Professional Certifications. The role of digital badges, micro/macro badges and credentials

Development of cybersecurity workforce development with stackable pre-apprenticeship and registered apprenticeship programs to utilize the "learn and earn" model and On the Job Training (OJT).

The role of non-traditional pathways Cybersecurity capability and skills gaps and diversity, equity, inclusivity, and accessibility issues will persist until we have an additional pathway into cybersecurity employment that does not pass through STEM dominated undergraduate and degree programs, often with heavy mathematics (i.e. Calculus) and science course requirements.

The importance of increased recruiting and support of new prospective cybersecurity students and workforce from all areas, backgrounds, and walks of life.

A Cybersecurity Career Education Non-Traditional Pathway Introduction

Report Section 3: K-12 Education and Section 4: Higher Education discussed in detail the value and design of a cybersecurity career education pipeline and pathway. Cybersecurity education pipeline and pathway components were discussed from kindergarten through doctoral degrees. Those sections (and several future sections) tie together the integral aspects of a cybersecurity career education preparation process through a variety of key recommendations made to policy and lawmakers in this report. It is essential to align and link cybersecurity education programs, industry based professional certifications, and work experience together to prepare qualified

and skilled cybersecurity professionals found across many NICE designated work roles and reduce cyber capability and skills gaps.

And while the current primary paradigm in cybersecurity professional preparation frequently relies on undergraduate and graduate degrees position minimum requirements, that has been changing in recent years. A reliance of STEM based cybersecurity (often hard sciences and technical degree programs) is widely considered a bottleneck in cybersecurity career preparation, and employers are becoming more willing to consider hiring talent on the basis of demonstratable skills (like cyber academies & bootcamps) as well as workforce development opportunities (like apprenticeships and internships).

The Value of Cybersecurity Non-Traditional Pathways

Critical Question 1: What is the best approach to cybersecurity workforce and career preparation? An academic or a skills-competency based approach? Both?

Do those with STEM based undergraduate degrees perform better in the cybersecurity profession than those without these degrees? Are 4-year degree holders better prepared for success in the cyber field than those with only work experience, professional industry-based certifications, training academies, and boot camps? What about the value of demonstratable skills and competencies as a key predictor of potential employee success in the cybersecurity domain and various workforce roles?

Critical Question 2: What is the value of a “traditional” and “non-traditional” pipeline/pathway into cybersecurity careers?

This question has become a key point of contention among cybersecurity workforce development experts, industry, academia, and policymakers. There is always the ongoing debate on the relative value of higher education (i.e. 4-year degree minimum job requirements) to predict employee success within the cybersecurity field. This is an important question to resolve through cybersecurity education program data collection, effective benchmarking, maturity model development, and deep-dive evaluation studies to drive sound legislation and prudent policy creation coupled with necessary financial support to make this happen. Regrettably, there has been very limited inquiry on this question little apparent research, evaluation, or analysis to guide this discussion in a fruitful way moving forward yet.

Non-Traditional Cybersecurity Career Education Pathway Components

K-12 Career Technical Education (CTE) Programs- Middle School/High School

Dual Enrollment Programs (in collaboration with Community Colleges)

Adult School Programs

Cybersecurity Academies, Bootcamps

Industry Based Professional Certifications

Cybersecurity Workforce Experience- Registered Apprenticeships, Internship Programs

Cybersecurity Professional Development and Networking Opportunities

Section 5 Conclusion

Cybersecurity non-traditional career pathways are a key tool to utilize in the long-term and sustained reduction of national cybersecurity capacity and skill gaps. This non-traditional pathway is an important and meaningful strategy to reduce and overcome numerous barriers in the cybersecurity workforce development and education barriers like cost, access, and program availability across geographics. These issues are addressed through the smooth operation of a non-traditional cybersecurity education approach that includes a cybersecurity pre-apprenticeship and registered apprenticeship model of workforce development. Pre-Apprenticeship and Registered Apprenticeship programs are growing in popularity and numbers nation-wide. Apprenticeships is a key strategy for cybersecurity workforce development and education in the traditional and non-traditional pathways. We must find and encourage cybersecurity education and workforce opportunities for students from all backgrounds, particularly those models that support the "earn and learn" approach of non-traditional cybersecurity career pipelines and pathways.

Diversity, Equity, Inclusivity, and Accessibility (DEIA) and supporting special populations concerns must be addressed for cybersecurity workforce preparation. The subject of DEIA in cybersecurity workforce development and education is found in the following report section.

SECTION #6

Diversity, Equity, Inclusivity and Accessibility (DEIA): Supporting Special Populations-

Prepared By

Emily Harris, CISSP, Higher Education Cybersecurity Professional

Section 6 Overview

This section addresses incorporating diversity, equity, inclusion, and accessibility practices into the education, recruiting, and hiring of Cybersecurity professionals. It will also address the non-traditional paths that are available to individuals seeking a career in Cybersecurity, and how those non-traditional paths can enhance and support the traditional, technical Cybersecurity skillsets. This section will highlight the importance of establishing and maintaining a diverse workforce and provide recommendations for improving the diversity of the Cybersecurity Workforce.

Defining the problem: Organizations prioritize advanced degrees in computer science and certifications - this is expensive and "prices out" lower income individuals from education and careers in cybersecurity.

Why this is important:

- Broadest range of opportunity to help resolve the workforce gap
- Diversity of ideas and opinions leads to solving complex problems
- Healthy conflict and disagreement

Diversity, Equity, Inclusion, & Accessibility Defined

White House Executive Order #14035 provides a definition of DEIA, summarized as:

Diversity – the practice of including the many communities, identities, races, ethnicities, backgrounds, abilities, cultures, and beliefs of the American people, including underserved communities.[19]
Equity – consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment.
Inclusion – recognition, appreciation, and use of the talents and skills of employees of all backgrounds.

[19] Diversity is not limited to traditional notions of race and gender. It also includes geographic diversity, neurodiversity, different types of physical ability, age, and those from different socioeconomic, religious, political, familial, and educational backgrounds.

Accessibility – design, construction, development, and maintenance of facilities, information and communication technology, programs, and services so that all people, including people with disabilities, can fully and independently use them.[20]

The United States is made up of a diverse population. In 2022 U.S. citizens were 58.9% white, 12.6% black, 19.1% Hispanic/Latino, and 6.1% Asian.[21] Further, 58.5% of the workforce is female.[22] And yet, according to a 2023 survey of United States Cybersecurity Analysts, 65.7% are white, 9.2% are black, 9.0% are Hispanic, 9.6% are Asian, and only 21.5% are women.[23] The Cybersecurity workforce does not accurately reflect the makeup of the nation, particularly with representation of blacks, Hispanics, and women. Providing the best protection against Cyber-attacks requires a workforce that reflects the diverse makeup of the American people.

Applications to Cybersecurity

Building a robust, sustainable Cybersecurity Workforce to combat threats requires workers that represent our communities and citizens. Cybersecurity threats impact all industries and all individuals. Effective threat prevention, detection, and remediation requires understanding the different kinds of threats that impact us. Employees from different backgrounds can anticipate and mitigate threats that are unique to their communities.

There are three key advantages to a diverse workforce to help keep the United States and its industries safe from Cybersecurity threats: 1) recruiting from the largest possible pool to close the Cybersecurity workforce gap; 2) promote innovation and improve problem solving; and 3) create healthy conflict and disagreement.

Recruiting from a Large Pool

The Cybersecurity workforce gap requires efforts to recruit from the largest pool feasible. This requires posting positions that will attract many different types of candidates to apply. According to the 2023 ISACA State of Cybersecurity Report, 38% of entry level Cybersecurity positions take 3 – 6 months to fill and 14% of non-entry-level positions take more than six months to fill. Part of this is inefficiencies in the hiring process, but a contributing factor is the lack of qualified candidates who apply.[24] Taking steps to make positions more attractive to

---

[20] Executive Order (EO) 14035, Diversity, Equity, Inclusion, and Accessibility (DEIA) in the Federal Workforce (June, 2021).
[21] https://usafacts.org/ U.S. Census Bureau, 2022
[22] U.S. Census Bureau, 2018-2022, 16+
[23] https://www.zippia.com/cyber-security-analyst-jobs/demographics/
[24] According to the ISC2 Global Workforce Study, 41% of worldwide companies cite lack of qualified talent as a significant factor in their Cybersecurity personnel shortages. https://www.pewresearch.org/science/2021/04/01/stem-jobs-see-uneven-progress-in-increasing-gender-racial-and-ethnic-diversity/

diverse and underserved populations contributes to creating a competitive pool of qualified, prospective employees.

Promote Innovation and Improve Problem Solving

Counteracting Cybersecurity threats requires innovative thinking to develop new strategies and tools that thwart and surprise Cyber attackers. Responding to incidents requires problem solving to find and stop the source of an attack and effectively minimize harm, investigate, and recover. Both innovation and complex problem solving require new ideas and new perspectives. Diverse teams increase the range of creative and new ideas, as they bring a range of experience and viewpoints into these activities. Homogenous teams, on the other hand, tend to fall into comfortable and common ideas and can easily stagnate.

Create Healthy Conflict and Disagreement

A natural outcome of bringing together employees with different backgrounds and viewpoints is the tendency to increase conflict and disagreement while working together. When leaders and project managers manage this conflict effectively, it gives rise to innovative solutions to complex problems by promoting negotiation to find common ground, fostering new ideas that are acceptable to all, and when managed effectively, a way of drawing teams closer together and improving group productivity.

Linkages and Alignment for Nontraditional Paths

Closing the Cybersecurity workforce gap requires recruiting and hiring from the broadest range of qualified individuals possible. The traditional path of formal education, training, and certification still remains an important pathway for job placement in the field. However, a significant percentage of the current Cybersecurity workforce does not have formal education in Cybersecurity, Information Technology, or other scientific disciplines. According to the 2023 ISC2 Global Cybersecurity Workforce study, out of cybersecurity professionals new to the field, 52% came from non-cybersecurity IT positions, 51% earned a certification and 31% received a bachelor's degree in Cybersecurity.[25] This means the majority of new Cybersecurity professionals did not launch their career with an undergraduate degree in the field. This bolsters the findings and recommendations from Section 5 on "Non-Traditional" Cybersecurity Career Education Pipelines and Pathways.

As discussed in other areas of this report, there are barriers to formal education, including the availability of Cybersecurity academic programs throughout the United States. Further, individuals may be interested in obtaining a degree in the field but do not have the financial

[25] 2023 ISC2 Cybersecurity Workforce Study - https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

means to attend a college with a relevant major. Financial insecurity often limits a student's option to local schools that may not have relevant majors.

Cybersecurity has a broad range of roles including Project Management, Portfolio Management, Leadership, Awareness and Training, and Technical Support. Individuals with degrees in Education would be qualified to conduct Security Awareness Training. A Psychology degree provides skills in evaluating user behavior and predicting future potential threats. Political Science or International Affairs students have backgrounds that bring a deeper understanding of the national security aspects of Cybersecurity and the global threats that come from nation states. A Liberal Arts education teaches students to think creatively, critically, and innovatively, which improves quick problem solving for incident response and investigations.

Section 6 DEIA Recommendations

There are several recommendations for organizations to put into place in order to improve the diversity of the Cybersecurity workforce. As the composition of the workforce changes, maintaining equity, inclusion, and accessibility is key to ensuring that a diverse workforce is accepted into workplace culture and the employees are kept happy and productive.

Write attractive job descriptions

Create job descriptions that focus primarily on the critical skills needed for the position. Avoid listing too many recommended skills that may dissuade candidates from applying. Emphasis all the benefits that come with the position, such as tuition assistance, retirement plans, health insurance, hiring bonuses, professional development, and re-location costs. Include diversity statements at the end of the description that encourage under-represented groups to apply. Consider hiring entry-level positions that do not require extensive experience, relevant degrees, or certifications and develop pathways for employees in those positions to advance.

Blind hiring practices

Blind hiring practices are those that remove any information that could lead to conscious or unconscious bias during the hiring process. One component of this process is to conduct all first interviews by phone only, to eliminate seeing a prospective employee and making determinations about their ethnicity, culture, or physical disability. Another common practice is to have a HR employee de-identify resumes prior to submitting them to the search committee for review. The resulting resume would just include skills and professional experience that are directly related to the role, and remove any indicators of race, culture, age, education, or other factors that are not pertinent to objectively evaluating a candidate's skills.

Cybersecurity workforce marketing

Marketing and public relations materials that are used to advertise and recruit Cybersecurity professionals should include representative, diverse individuals. Individuals are more attracted to positions that appear to be populated by those who look like them or match their values.

Representation in teaching and learning

Teachers from diverse backgrounds bring different experiences and ideas into teaching. Also, similar to marketing, representation in education inspires confidence that minority populations can succeed in the profession. This applies to Cybersecurity education at all levels and other training programs.

Fund programs in schools with minority populations

Create funding mechanisms to support Cybersecurity education programs in school districts in underserved communities.

Expand remote work opportunities or offering re-location funds

Many minority population are barred from job opportunities because they are located in population centers that are cost-prohibitive to live in or near. Post-COVID, more organizations have hybrid or remote opportunities. However, many companies have reverted to 100% on-site work policies and should re-evaluate the feasibility of opening remote roles. Many Cybersecurity roles are conducive to remote work, particularly in software development and application engineering. Remote work can also better accommodate certain kinds of physical differences and neurodivergent employees. Further, remote opportunities help close the Cybersecurity gap by recruiting employees from a geographically broad pool. If an organization absolutely cannot accommodate remote work, consider offering re-location funds to encourage non-local candidates to apply and support those with limited financial means.

Internal transitions to Cybersecurity teams

Recruit individuals from other areas of the organization to move into Cybersecurity roles. Employees who are currently employed at an organization already have deep institutional knowledge that they can immediately apply to a new Cybersecurity role. Many workers may have technical ability but did not pursue a technical education or profession due to actual or perceived barriers to access, which means they can be trained for a new role with minimal investment. Also, as previously mentioned, individuals with other forms of education and majors can fill many Cybersecurity roles with additional training to close existing skills gaps. Information Technology employees from the Help Desk, Networking, and System Administration already have most of the key skills required for Cybersecurity, and it may be easier to backfill those positions than recruit directly for Cybersecurity roles.

Make events accessible for disabled individuals

Educational opportunities such as hackathons, “capture the flag,” and other hands-on activities mentioned in previous sections should be accessible to those with disabilities. The events should be held at ADA compliant locations, offer ASL interpretation for the deaf and hard of hearing, and be open to accommodating special requests from registrants for other unique needs, such as quiet or low-light spaces.

Provide government funding to support organizations targeting diverse communities

There are many non-profit organizations that encourage and support diverse and underserved communities in computing. These organizations sponsor networking events, promote job opportunities, host events, perform outreach, provide mentoring, and conduct other activities to support and encourage minorities to enter and persist in technical fields. The government could create new funding through NSF grants to expand these organizations into broader public relations activities such as assemblies at the K-12 level or hosting career fairs for High School seniors. Grants could also be given for technical education outside the classroom or training programs for Cybersecurity certifications.26

Encourage Computer Science and Cybersecurity programs at specialized institutions

Target Historically Black Colleges and Universities, Women's Colleges, Religious Schools, and other specialized Higher Education institutions for developing new Cybersecurity academic programs. Include support for post-graduate job placement by creating partnerships with Cybersecurity or Technology firms for internships and externships.

Section 6 Conclusion

White House Executive Order #14035 states that the "Federal Government should have a workforce that reflects the diversity of the American people. A growing body of evidence demonstrates that diverse, equitable, inclusive, and accessible workplaces yield higher-performing organizations." These principles should be applied to recruiting Cybersecurity professionals into the workforce to enhance the nation's Cybersecurity defense posture and help reduce the harm of Cyber-attacks that are a constant threat to both individual organizations and national security. Implementing the preceding recommendations will help achieve the goal having a workforce that accurately reflects the citizenry that United States strives to protect.

Additional DEIA Recommendations:

- Hiring practices
- Recruiting from non-technical fields and investing in professional development
- Sponsoring for certs
- Fund programs in schools with minority populations

---

[26] Organizations supporting diversity in technical fields: https://www.cio.com/article/193688/professional-organizations-focused-on-diversity-in-tech.html and organizations supporting women in technical fields: https://www.cio.com/article/215709/16-organizations-for-women-in-tech.html

- Representation in teaching and learning
- Girls who Code, Women in Cybersecurity

Reference list:

- https://www.isc2.org/research - global workforce student and women in cybersecurity 2018 study
- https://www.aspeninstitute.org/wp-content/uploads/2021/09/Diversity-Equity-and-Inclusion-in-Cybersecurity_9.921.pdf - aspen institute
- https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/Innovation-Through-Inclusion-Report.pdf - 2018 ISC2 and Frost and Sullivan report
- https://www.accenture.com/content/dam/accenture/final/capabilities/technology/security/document/Accenture-Rising-to-the-Top-Accenture-Cybersecurity-Forum.pdf#zoom=50 - 2022, discusses the issue and why it is important
- https://www.pewresearch.org/science/2021/04/01/stem-jobs-see-uneven-progress-in-increasing-gender-racial-and-ethnic-diversity/ - general stats for STEM fields 2017-2019
- https://ncses.nsf.gov/pubs/nsf23315 - NSF STEM data 2022 (note women have the least percentage of math/computing degrees)
- https://eric.ed.gov/?id=EJ895873 - 2010 Department of Education study on increasing minority participation in Computer Science
- https://iacis.org/iis/2013/189_iis_2013_143-152.pdf - more background on the problem, 2013
- https://www.cio.com/article/201905/women-in-tech-statistics-the-hard-truths-of-an-uphill-battle.html - good summary of statistics generally and points to other articles, general in IT, not specific to Cybersecurity

SECTION #7

Cybersecurity Workforce Preparation- The Value of Industry Recognized Professional Certifications

Prepared by:

Jeff Angle, Senior Director, Academic and Workforce Development, ISACA

Section 7 Overview

There are two key objectives to the discussion of value of professional certifications found in this section.

1. Link and align cybersecurity education/training programs of study with needed industry recognized professional certifications to meet employer hiring and retention needs.

2. Build a framework and road map for stackable IT-Cybersecurity Certifications for entry-level, intermediate, and advanced work roles.

Role of Certificates

Over the last decade, many public community colleges and other regional institutions have expanded their applied and technical programs to offer more accessible and affordable options for students. Learners are looking for more flexible options that can directly deliver the technical skills they need in the workforce. In the 2020–21 academic year, undergraduate credential earners increased 1.1% from the number reported the previous two years. This growth largely came from students with prior qualifications who were stacking credentials. Students are often taught at an early age how to break big jobs down into smaller, manageable tasks to reduce procrastination and make their goals seem more realistic and reachable. This concept of learning via micro-productivity is increasingly used in today's business world to keep skills updated.

Often referred to as stackable micro-credentials and credentials, this method provides shorter and more highly focused programs that enable learners to gain and validate knowledge and skills in a faster time frame. A micro-credential or credential can be used to gain expertise in a specific area, or a learner can build up ("stack") a series of micro-credentials as a pathway to a larger certification, degree or career opportunity. Stackable micro-credentials and credentials are also an effective pathway for lifelong learning. Enterprises use them to fill skills gaps, identify qualified candidates and increase staff morale. Individuals, whether new to the workforce, recently graduated, changing careers, or going back to work after an extended break, are using them to gain skills at their pace in high-demand fields. These credentials have encouraged institutions to be intentional with how they build their program pathways and expand their academic portfolios. These shorter-term credential pathways allow individuals the

opportunity to progress from one credential type to the next within the same institution, continuously building upon the skills or knowledge topic.

Findings from several state studies have shown that 32% to 43% of non-degree certificate earners are re-enrolling in college and stacking credentials. Among those who participate in stacking credentials, most also went on to earn a degree. In 2021, RAND Corporation conducted a study of the Ohio workforce and examined statewide educational records, focusing on stackable credentials. The goal was to evaluate how stackable credentials can make postsecondary education and training more accessible to individuals who didn't want traditional college degree programs. The study found that Ohio experienced strong growth in short-term credential programs over the last 15 years, particularly in the healthcare (146%) and manufacturing and engineering technology (171%) fields. In addition, these certificate programs reported more stackable features over time, with more than half being new Manufacturing and Engineering Technology (MET) and IT certificate programs. 6 (RAND, 2021).

Generational changes, an evolving economy and shifts in the global marketplace have dramatically increased the demand for flexibility in how to approach education, skills-building and career advancement. To fill these needs and gain the benefits of microproductivity in a time- and cost-efficient manner, academic institutions can partner with an established provider of quality certificates and certifications such as ISACA, EC-Council, and ISC2, professional associations in IT audit, risk, cybersecurity, privacy, ethical hacking and governance that have for 50+ years equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations and build a more trusted and ethical digital world. Over the last decade, companies and universities have increasingly entered research deals that offer invaluable benefits to both the employers and institutions, such as early-stage research and recruitment, content development and corporate sponsorships. Tech giants that originated on the West Coast have established East Coast headquarters over the years. Facebook, Twitter and Amazon have all opened new HQs and R&D offices across the institution-heavy East Coast. These partnerships highlight the importance of direct employer collaboration to produce successful long-term relationships and opportunities for four-year colleges and universities.

In its 2023 study of employers, UPCEA partnered with Collegis Education to conduct a survey to better understand how they perceive external partnerships with higher education institutions and associations. Overall, the number of respondents whose companies have existing external partnerships with organizations or institutions increased from 54% in 2022 to 68% in 2023. Of respondents from companies that partner with four-year colleges or universities, 33% said the main reason is for employee development, 28% said recruitment and 12% cited access to quality staff/resources/programs. Responses mentioned fewer than four times were placed in the "Other" category and included student rotations, cost effectiveness, and to help the community and educate students, among others. When participants were given a list of reasons for companies to partner with a college or university, 76% said the quality of content, 69% the

reputation of the institution, 46% affordability, 45% the ability to get college credit for courses and 45% having previous experience with the institution. Seventy-three percent of respondents said their partner colleges or universities create custom programming for their organizations, either most of the time (47%) or all the time (26%), while 25% said custom programming is created some of the time.

When asked why their organizations would want to continue partnerships with colleges and universities, 77% of respondents said these institutions meet their needs, 71% said they have positive employee feedback and 68% said they have seen improved job performance Based on these findings, employers find value in partnerships with colleges and universities to develop professional development programming. By collaborating on the creation of stackable pathways, institutions can develop partnership programs to create stackable credentials in various subject areas and will have the unique ability to cater their certificates and courses toward skills that can be directly applicable to in-demand occupations.

Stackable Credentials

Stackable credentials can provide value to individuals employed in all types of careers, and those working in the IT industry are no exception. New technological innovations are changing the way in which business is conducted. As a result, the IT industry is growing at an expected compound annual growth rate of 8.4% from 2022 to 2023. Emerging technology companies are expected to grow at a rate of 104% worldwide, followed by software companies at 50% (Statista, 2023). With the dominance of the IT industry and the necessity of technical skills, companies are encouraging their employees to develop the skills necessary to continue to innovate upon the technological advances that are fueling this market growth. Much of this adult learning can be found in internal workshops, professional development partnerships and professionals returning to school. Recent data indicates this to be the case; a study conducted by Pluralsight, a technology workforce development company, found that 72% of tech leaders plan to increase their investment in tech skills development despite economic uncertainty. This focus is not only being adopted by employers but also by employees. Another study by the same company found that 48% of tech workers consider changing jobs due to a lack of upskilling resources. These studies suggest that upskilling is being heavily sought after for long-term success within the IT industry.

Stackable credentials are the optimal way to upskill, and ISACA, EC-Council, CompTIA, and ISC2 offer many programs that teach core competencies specifically relevant to IT. For example, learners looking to move into IT may want to start their stackable journey with ISACA's Cybersecurity Fundamentals certificate or CompTIA's SEC+ which was developed for students, recent graduates, individuals or teams looking to upskill and rising IT professionals. The certificate combines knowledge and practical, hands-on learning, enabling candidates to demonstrate their understanding of the principles that frame and define cybersecurity, and the integral role of cybersecurity professionals in protecting enterprise data. Instructors are industry-certified current practitioners who share proven techniques and expertise. Learners

may continue with specialty certificates in areas such as artificial intelligence (AI), blockchain, cloud and other areas. After gaining this knowledge and combining it with work experience, they may decide to progress to earning in-demand certifications, as Certified Information Systems Auditor ® (CISA ®), Certified Information Security Manager ® (CISM ®) or Certified CISSP, CYSA+, or CEH.

In addition to this linear growth, learners may choose different pathways during different phases of their careers. At some point they may want to take advantage of their knowledge and move to a related area that requires additional specialized knowledge. For example, a cybersecurity professional may want to move into compliance, or IT audit, or move into or out of the GRC space before trying more technical roles. ISACA's stackable credentials help those people move into the new area with a globally recognized program to expand and validate their skills. Throughout the journey, these professionals gain solid insights into many areas that will help them increase their options for promotions and/or career changes. Stackable certificates are also vital to staying ahead of the lightning-fast tempo of technology. Cloud computing, for example, has expanded over just a few years to focus on hyperscale cloud, and professionals now need to know how to bring multiple cloud providers together at scale. They also need to know how to audit these new structures and ensure their organization has optimal risk and governance postures. Keeping up with this pace requires a strong partnership among learning institutions, student learners and professional associations.

While ISACA specializes in the IT and digital trust space, organizations and individuals in many industries and sectors also benefit from Stackable Certificates. Technology organizations are leading the way, but other professions are involved in innovative initiatives, too. One of these industries is manufacturing as highlighted by the change in educational trends among manufacturing employees. Before 2005, workers with a high school diploma or less held the largest number of good jobs in manufacturing. However, from 1991 to 2016, the number of employees with bachelor's degrees increased from 2.8 to 3.6 million. These figures indicate that the desire for education within the manufacturing industry has increased significantly. Additional evidence for this underlying theme can be seen in new research in England that reveals that in 2022, 80% of workers in the manufacturing and utilities industry are interested in learning new work skills. 27 The top areas workers wanted to explore included IT and digital (20%), finance (16%) and business (16%) (UPCEA, 2023). In the same way that new technologies are proliferating throughout the corporate world of IT, new technology is spreading throughout the manufacturing industry, creating opportunities to develop more efficient processes that make employees who have the skills to utilize those processes more valuable. There are numerous options to develop the skills to capitalize on this trend, and stackable credentials provide one of the best strategies. One set of opportunities for upskilling is offered by Smart Automation Certification Alliance (SACA).

SACA offers four certifications designed for workers or students in high school or college, which cover competencies including basic operations, advanced operations, robot system operations and networking and data analytics. Obtaining certifications like these will enable students to

be prepared to enter a rapidly evolving workforce and achieve success quickly. In addition to the manufacturing industry, the healthcare industry also has opportunities for upskilling through stackable credentials, particularly within digital technologies.

In a study conducted by Healthcare and Information and Management Systems Society (HIMSS®), 80% of health systems plan to increase their investment in digital tools over the next five years. This figure is related, in part, to the increased urgency brought on by the COVID-19 pandemic to offer virtual healthcare services, since the supply of doctors and nurses was significantly less than the demand. According to a survey conducted by Local Circles during the first wave of COVID in India, only 4% of patients who needed an Intensive Care Unit (ICU) bed were able to find one, while 78% used connections in the hospital to secure a bed. This disparity highlights the need for hospitals to have the ability to deal with a sudden surge of demand for healthcare by offering digital services for care not requiring in-person interaction.

The technologies that stand to be at the forefront of this digital revolution in healthcare include virtual consultations, wearable technology that assists with monitoring vital signs continuously and artificial intelligence, among others. In a survey of pharmaceutical companies (UPCEA (2023), the most cited emerging technologies in which they invested were digital media (53%), AI (51%), social media (51%) and big data (50%). The skills that are important for upskilling in the information technology industry are also important in the healthcare industry, and upskilling can be obtained through stackable credentials to equip employees with the ability to utilize these new technologies.

Regardless of industry, stackable credential programs can be a great bridge between academic programs and the industry-intensive certification programs for mid- and senior-level professionals. Students who want to advance in their careers may not be able to go back to school full time or may even struggle to learn at the same pace as students at traditional institutions. A 2023 disengaged learners study conducted by UPCEA and StraighterLine (UPCEA & StraighterLine, 2023) showed that if an institution offers alternative or micro-credentials that are stackable, over three-quarters (76%) of respondents said that this would greatly increase or increase their interest in pursuing an undergraduate degree.

Section 7 Certification/Credential Recommendations

There are four key recommendations related to industry based professional certifications and credentials and leveraging their value in the cybersecurity professional preparation and retention processes.

1. Perform comprehensive curriculum mapping and analysis to document the types of key knowledge, skills, and competencies found in cybersecurity (and related professional industry recognized certification programs; and how certifications link together in a vertical alignment of foundational, beginner, intermediate, and advanced certification and credential programs.

2. Develop an industry based professional certification framework and "road map" which stackable certificates and credentials are linked across work roles throughout the career ladder from preparation, entry level, intermediate, and advanced work roles in cybersecurity.

3. Promulgate policy guidance to tightens the process by which professional and academic certifications are fused together credit, non-academic, and digital badging (microbadges/ micro-credentials) as options and offerings at K-12, Colleges, and Universities.

4. Analyze, evaluate, and develop a "non-traditional" cybersecurity career education pathway utilizing industry recognized professional certifications, linked with pre-apprenticeship programs and registered apprenticeships at a national and state level as a key training modality in cyber professional careers across all NICE Workforce Framework domains and work roles.

Sources:

Abraham, L. (2023, September 14). *Strengthening the manufacturing workforce in Ohio*. RAND. https://www.rand.org/pubs/research_reports/RRA2517-1.html

Etter, B., Fong, J., Sullberg, D., Wang, K., Zovko, A., & Angle, J. (2024, January 17). *Flexible, Stackable Certificates: The Future of EducatioN*. UPCEA. Retrieved January 25, 2024, from https://upcea.edu/wp-content/uploads/2023/12/Flexible-Stackable-Certificates-The-Future-of-Education_UPCEA-and-ISACA_December-023.pdf?utm_source=Marketing&utm_medium=Email&utm_campaign=UPCEA&_zs=HLiud&_zl=iRct3

https://www.insidehighered.com/news/2023/04/03/majority-americanslack-confidence-value-four-year-degree

https://www.wsj.com/articles/americans-are-losing-faith-in-collegeeducation-wsj-norc-poll-finds-3a836ce1

https://www.govtech.com/education/higher-ed/universities-softwaregiants-partner-on-tech-upskilling

https://www.highereddive.com/news/credential-stacking-drove-11- increase-in-undergraduate-degrees-earned-las/625912/

https://hbr.org/2018/01/why-companies-and-universities-should-forgelong-term-collaborations

https://collegiseducation.com/resources/effect-of-employerunderstanding-and-engagement-non-degree-credentials/

(2023). *Adressing Employer Barriers to Engage with Institutions"* (1st ed.). UPCEA & Collegis. https://collegiseducation.com/resources/effect-of-employerunderstanding-and-engagement-non-degree-credentials/

https://www.globenewswire.com/news-release/2023/05/11/2667047/0/ en/The-Information-Technology-Industry-is-Expected-to-Growth-at-aRate-of-More-Than-8-During-The-Forecast-Period-2022-2032-By-TheGlobal-Market-Model.html

Statista. (2023, July 7). *IT industry growth rate forecast worldwide from 2018 to 2023, by segment*. https://www.statista.com/statistics/967095/worldwide-it-industry%20growth-rate-forecast-segment

Nelson, M. (2021, December 1). *New research answers question every college wants to know: Why do students leave and how do we get them back?* UPCEA. https://upcea.edu/new-research-answers-question-every-college-wants-to-know-why-do-students-leave-and-how-do-we-get-them-back/

SECTION #8

Cybersecurity Workforce Preparation—On the Job Training

Prepared By

Patrick Slattery, Director of Industry Engagement, Zicklin School, Baruch College, City University of New York (CUNY)

Cybersecurity OJT Objectives

The Experiential Learning Theory (ELT), as outlined by Kolb in 1984, highlights the significance of experiential engagement in the educational journey. This theory differentiates itself from cognitive learning theories by prioritizing experiential engagement over cognitive and behavioral approaches. Moreover, ELT proponents argue that learning should be viewed as a dynamic process rather than solely focusing on the outcomes of instruction and formal assessments. According to this theory, learning involves revisiting previous knowledge, resolving discrepancies, adopting a comprehensive and adaptable approach, and emerging from the dynamic interaction between the individual and an environment to generate new knowledge.

On-the-Job Training (OJT) is a frequently used mechanism for experiential learning in cybersecurity. The predominant outcomes that OJT training can be expected to produce for a student interested in a career in cybersecurity include the following items:

1. Practical Skill Acquisition
2. Application of Theoretical Knowledge
3. Problem-Solving Skills
4. Professional Networking
5. Understanding of Workplace Dynamics
6. Adaptability to Technological Changes
7. Career Clarification and Direction
8. Enhanced Employability
9. Development of Professional Ethics
10. Feedback and Personal Development
11. Actualizing the Value of Inclusivity and Support for Neurodiversity

1. Practical Skill Acquisition: OJT in cybersecurity enables students to develop practical, hands-on skills that are crucial in this field. This includes understanding real-world applications of cybersecurity principles, tools, and techniques. This outcome can seem obvious and is often top-of-mind to employers as they review the experience and demonstrated skills of candidates.

2. Application of Theoretical Knowledge: Students can apply theoretical concepts learned in academic settings to real-world scenarios. This bridges the gap between academic understanding and practical application, enhancing their comprehension and retention of cybersecurity concepts. A significant number of cybersecurity students lack an understanding of the context and complexity of operational situations where the concepts they learned are applied. For students who have not worked in a large, complex enterprise the application of theoretical knowledge can often be naively oversimplified. Some students who have had the benefit of being raised amongst family members with experience in large, complex organizations may have a basic understanding of the application of cybersecurity practices across multiple organizational units and thousands, or tens of thousands of users/employees, but that basic understanding is not sufficient for the expectations of most employers. OJT can help bridge this understanding gap.

3. Problem-Solving Skills: Exposure to actual cybersecurity challenges during OJT fosters critical thinking and problem-solving skills. Students learn to navigate and resolve complex cybersecurity issues, which is a vital skill in this ever-evolving field. Not every cybersecurity incident plays out in textbook fashion or well-practiced exercises and case studies. OJT helps hone the analytical skills required to meet the dynamic challenges of this threat landscape.

4. Professional Networking: OJT provides opportunities for students to build professional networks within the cybersecurity community. These connections can be invaluable for future career prospects and professional guidance. Professional relationships can help to build confidence and provide students with trusted mentors and coaches. As part of the drive to increase diversity in the cybersecurity workforce, OJT opportunities to network across a diverse community of professionals, and provide excellent role models and motivations for students to succeed within the field and ecosystem.

5. Understanding of Workplace Dynamics: Students gain insight into the workings of cybersecurity roles within organizations. This includes understanding team dynamics, organizational structures, and the practical aspects of working in cybersecurity. Students emerging from an academic environment can find the nuances and energies of workplace dynamics daunting. OJT and the networking opportunities already described provide invaluable insight into the various informal structures and relationships that are critical to career success.

6. Adaptability to Technological Changes: Cybersecurity is a rapidly evolving field. OJT allows students to experience and adapt to new technologies and methodologies, keeping their

skills relevant and up to date. Learning a range of currently popular cybersecurity tools is certainly valuable but those skills can be enriched with the ability to learn to understand and adapt to different technologies, both old and new. OJT provides an opportunity to exercise adaptability and continuous learning.

7. Career Clarification and Direction: Through OJT, students can better understand various career paths within cybersecurity, helping them to make informed decisions about their professional future. Frameworks, taxonomies, and research studies can provide informative static images of cybersecurity roles and career paths, but they typically lack nuance and can restrict vision and motivation. OJT gives students a pragmatic and dynamic view of where they can take their talents and skills to achieve success.

8. Enhanced Employability: Practical experience gained through OJT enhances a student's employability. Employers often seek candidates with real-world experience, and OJT provides students with a competitive edge in the job market. Historically, availability of established OJT offerings was often limited to a privileged population of legacy students from affluent homes and parental support that leveraged professional and social networks. Expanding the number and availability of OJT offerings can throw open doors to opportunities on a more egalitarian basis and raise both the number and caliber of students pursuing successful careers in cybersecurity.

9. Development of Professional Ethics: Exposure to real-world cybersecurity environments allows students to understand and develop the professional ethics required in this field, including confidentiality, integrity, and the responsible use of information. Case studies and class exercises tend to present ethical decisions in stark contrast – the right choice, versus the wrong choice. In practice, cybersecurity professionals are rarely presented with such clear distinctions. Ethical decisions can be nuanced and subtle. They can also have knock-on effects that accrue over time. OJT can provide exposure to these more realistic scenarios and the perspectives and insights of professionals making decisions.

10. Feedback and Personal Development: OJT offers students the opportunity to receive direct feedback from experienced professionals, facilitating personal and professional growth and development in the cybersecurity domain. Assessments in academia help students to understand their level of achievement regarding conceptual models, facts, and reasoning methods. OJT enriches that understanding with constructive feedback from practitioners' experiences in more complex situations.

11. Actualizing the Value of Inclusivity and Support for Neurodiversity: A significant challenge is ensuring that On-the-Job Training (OJT) programs are inclusive and supportive of neurodivergent individuals, both as students and as professionals within the cybersecurity field. Neurodiversity encompasses a variety of neurological differences, including but not limited to autism spectrum disorders, ADHD, dyslexia, and others. These differences can affect how individuals learn, communicate, and interact within professional environments.

Effectiveness of On the Job Training

To evaluate the effectiveness of On-the-Job Training (OJT) programs in cybersecurity the following areas of performance measurement can be considered:

1. Job Offer Rate Post-Training
2. Skill Competency Assessments
3. Retention Rates in Employment
4. Feedback from Employers and Industry Experts
5. Contribution to National Cybersecurity Goals

1. Job Offer Rate Post-Training: This is a direct indicator of an OJT program's success in making students employable. A high rate of job offers suggests that the training is relevant and valued by employers. It's important to track not just the quantity but also the quality of these offers – for instance, roles that align well with the training provided and positions within reputable organizations.

2. Skill Competency Assessments: Pre- and post-training assessments can provide quantitative data on the skills acquired by students. These assessments should be aligned with industry standards and the specific requirements of cybersecurity roles. Improvement in these assessments can indicate the effectiveness of the OJT in imparting necessary skills.

3. Retention Rates in Employment: Tracking the long-term employment stability of graduates can provide insight into the lasting impact of the OJT. High retention rates suggest that the skills learned are not only adequate for gaining employment but also for sustaining it. This metric also reflects on the program's ability to instill a deep understanding and adaptability in the rapidly evolving field of cybersecurity.

4. Feedback from Employers and Industry Experts: Regular feedback from employers who hire these students can offer qualitative insights into the OJT program's effectiveness. This could include the students' readiness for real-world challenges, their problem-solving abilities, and how well they adapt to the evolving nature of cybersecurity threats.

5. Contribution to National Cybersecurity Goals: Since OJT programs can be part of a national strategy, their effectiveness could also be measured against broader goals such as reducing the national cybersecurity skills gap, improving national cyber defense capabilities, or enhancing innovation in cybersecurity technologies. Metrics could include the number of graduates working in critical infrastructure sectors or their involvement in significant national cybersecurity initiatives.

Each of these methods provides a different perspective on the effectiveness of OJT programs, and together, they can offer a comprehensive understanding of how well these programs are preparing students for careers in cybersecurity.

On the Job Training Models

In the U.S., the following modes of On-The-Job (OJT) training are typically available to students. They are described in further detail below:

1. Apprenticeships
2. Paid Internships
3. Co-ops
4. Incumbent Workforce
5. Training
6. Customizable Workforce/Training Solutions
7. Complementary Programs and Resources

1. Apprenticeships: This mode of OJT involves a structured training program where students work under the guidance of experienced cybersecurity professionals. It combines practical, on-the-job experience with some formal educational components, allowing students to develop a deep understanding of cybersecurity practices and principles.

2. Paid Internships: Paid internships offer students the opportunity to work in a real-world cybersecurity environment for a limited period. This experience provides practical exposure to the field while also offering financial compensation, making it a mutually beneficial arrangement for both the student and the organization.

3. Co-ops: Cooperative education (co-ops) integrates academic learning with practical work experience. Students alternate between periods of classroom learning and working in cybersecurity roles. This model allows for the application of academic theories in real-world settings, enhancing the overall learning experience.

4. Incumbent Workforce: This training involves the upskilling or reskilling of an organization's existing workforce in cybersecurity. It focuses on enhancing the skills of current employees to meet evolving cybersecurity needs, ensuring that the workforce remains competent and capable in the face of new challenges and technologies.

5. Training: This encompasses various forms of structured learning experiences, ranging from workshops and seminars to comprehensive training courses. These programs are designed

to impart specific cybersecurity skills and knowledge, often focusing on tools, technologies, or methodologies.

6. Customizable Workforce/Training Solutions: This approach involves tailoring training programs to meet the specific needs of students or organizations. It allows for flexibility in learning objectives, methodologies, and outcomes, ensuring that the training is relevant and effective in addressing the unique challenges and goals of the participants.

7. Complementary Programs and Resources: These are additional educational resources and programs that supplement primary cybersecurity training. They can include online courses, webinars, conferences, and other learning materials that provide broader knowledge and insights, supporting the comprehensive development of cybersecurity students.

Cybersecurity OJT Challenges

The major challenges that the U.S. faces with respect to On-the-Job Training (OJT) of cybersecurity students can be categorized into several key areas. They are described in further detail below:

1. Bridging Academic and Operational Gaps
2. Ensuring Relevant and Up-to-Date Training
3. Access and Equality in OJT Opportunities
4. Quality and Consistency of OJT Programs
5. Integration with Academic Curricula
6. Measuring and Ensuring Effectiveness
7. Adaptability and Personal Development
8. Actualizing the Value of Inclusivity and Support for Neurodiversity
9. Professional Networking and Mentorship
10. Resource Allocation and Funding
11. National Cybersecurity Goals Alignment

1. Bridging Academic and Operational Gaps: One of the primary challenges is the significant gap between theoretical knowledge acquired in academic settings and its practical application in complex, real-world environments. Many students lack an understanding of the context and complexity of operational situations, which OJT aims to address. However, the effectiveness of OJT in bridging this gap varies, depending on the quality and relevance of the training provided.

2. Ensuring Relevant and Up-to-Date Training: Cybersecurity is a rapidly evolving field. A major challenge for OJT programs is to stay current with the latest technologies, threats, and industry best practices. This requires continuous updating of training materials and methods, which can be resource intensive.

3. Access and Equality in OJT Opportunities: Historically, OJT opportunities in cybersecurity have been limited and often accessible primarily to students from more privileged backgrounds. Expanding these opportunities to a broader and more diverse student population is crucial but challenging, requiring significant investment, and restructuring of existing programs.

4. Quality and Consistency of OJT Programs: The effectiveness of OJT programs can vary widely depending on the organization providing the training. Ensuring a consistent, high-quality training experience across different programs is a significant challenge. This includes maintaining a standard curriculum, experienced trainers, and relevant, hands-on experiences.

5. Integration with Academic Curricula: Coordinating OJT with academic programs to ensure a seamless integration of practical skills and theoretical knowledge is complex. This involves collaboration between educational institutions and industry partners, which can be hindered by differing objectives, capabilities, and resource limitations.

6. Measuring and Ensuring Effectiveness: Effectively measuring the outcomes of OJT programs, such as job offer rates post-training, skill competency, and long-term employment retention, is challenging. These metrics are crucial for evaluating and improving the quality of OJT programs but require comprehensive data collection and analysis.

7. Adaptability and Personal Development: While OJT aims to develop adaptability in students, the varying nature of cybersecurity roles and the rapid pace of technological change make it difficult to ensure that all necessary skills and competencies are covered. Additionally, personal development aspects such as professional ethics and problem-solving skills are harder to quantify and teach in an OJT setting.

8. Actualizing the Value of Inclusivity and Support for Neurodiversity: While OJT provides a potential outcome for both neurodivergent students and established professionals, it also poses a significant challenge to ensure that OJT programs are inclusive and supportive of neurodivergent individuals.

Neurodiversity encompasses a variety of neurological differences, including but not limited to autism spectrum disorders, ADHD, dyslexia, and others. These differences can affect how individuals learn, communicate, and interact within professional environments.

It is important to consider some of the following, key aspects of this challenge –

A. Leveraging Strengths: Most importantly, neurodivergent individuals often have unique skills and perspectives that can be highly beneficial in cybersecurity roles, such as pattern recognition, attention to detail, and innovative problem-solving. OJT programs need to recognize and leverage these strengths effectively.

B. Understanding and Awareness: There is often a lack of understanding and awareness about neurodiversity in the workplace, which can lead to misconceptions, biases, and barriers to effective collaboration and learning.

C. Accommodations and Adjustments: OJT programs may not always have the necessary accommodations or adjustments in place to support the unique learning and working styles of neurodivergent individuals. This can include modifications to communication methods, training materials, and assessment techniques.

D. Social and Professional Integration: Neurodivergent individuals may face challenges in social interactions and professional networking, which are key components of OJT. Ensuring that these aspects of training are accessible and inclusive is crucial.

E. Supportive Environment: Creating a supportive and understanding environment that promotes psychological safety and encourages open communication about individual needs and accommodations is essential.

9. Professional Networking and Mentorship: Although OJT provides networking opportunities, ensuring meaningful and lasting professional relationships is challenging. This is particularly important for fostering diversity and inclusion in the cybersecurity workforce.

10. Resource Allocation and Funding: Establishing and maintaining high-quality OJT programs requires significant financial and human resources. Securing consistent funding and allocating resources efficiently remains a major challenge, especially for public institutions and non-profit organizations.

11. National Cybersecurity Goals Alignment: Aligning OJT programs with broader national cybersecurity goals, such as reducing the skills gap and improving national cyber defense capabilities, requires coordination at multiple levels, including government, industry, and academia. This alignment is crucial but often difficult to achieve due to varying priorities and strategies among stakeholders.

Cybersecurity On the Job Training Opportunities

A strategic plan to address the major challenges in On-the-Job Training (OJT) for cybersecurity students could focus on practicality, resilience, and the common good as described below.

1. Bridging Academic and Operational Gaps:
    - Goal: Develop a standardized framework that integrates academic learning with practical application, ensuring that OJT programs align with real-world cybersecurity needs.
    - Action: Facilitate partnerships between educational institutions and industry leaders to co-create curricula that reflect current operational challenges.
2. Ensuring Relevant and Up-to-Date Training:
    - Goal: Continuously evolve OJT programs to keep pace with technological advancements, even when this requires significant changes to established systems.
    - Action: Establish a national cybersecurity OJT council responsible for regularly updating training standards and practices.
3. Access and Equality in OJT Opportunities:
    - Goal: Ensure equitable access to OJT programs for all students, regardless of background.
    - Action: Implement national policies that incentivize and support the creation of diverse and inclusive OJT opportunities.
4. Quality and Consistency of OJT Programs:
    - Goal: Balance the need for high standards with the practicalities of diverse training environments.
    - Action: Create a national accreditation system for OJT programs to maintain quality and consistency.
5. Integration with Academic Curricula:
    - Goal: Recognize the interdependence of academic and practical learning.
    - Action: Encourage joint ventures and collaborations between educational institutions and cybersecurity industries for curriculum development.
6. Measuring and Ensuring Effectiveness:
    - Goal: Fairly assess the effectiveness of OJT programs in preparing students for the cybersecurity workforce.
    - Action: Implement a national system for tracking and analyzing the outcomes of OJT programs, including employment rates and skill competency.

7. Adaptability and Personal Development:
    - Goal: Promote a culture of continuous learning and adaptability in the face of changing cybersecurity landscapes.
    - Action: Integrate modules focusing on adaptability, ethics, and critical thinking into OJT programs.
8. Actualizing the Value of Inclusivity and Support for Neurodiversity:
    - Goal: Establish a national framework for inclusivity in cybersecurity OJT programs that recognizes and leverages the strengths of neurodivergent individuals.
    - Action: Develop and implement comprehensive training for educators and employers on neurodiversity, focusing on creating adaptable and supportive learning and working environments within the cybersecurity field.
9. Professional Networking and Mentorship:
    - Goal: Balance technical training with opportunities for professional relationship-building.
    - Action: Establish mentorship programs and networking events within OJT programs, emphasizing the importance of community and support in the cybersecurity field.
10. Resource Allocation and Funding:
    - Goal: Allocate resources in a manner that maximizes the effectiveness and reach of OJT programs.
    - Action: Direct government funding and private sector investment in cybersecurity OJT programs, emphasizing their role in national security.
11. National Cybersecurity Goals Alignment:
    - Goal: Align OJT programs with national cybersecurity objectives to contribute to the greater good.
    - Action: Develop a national cybersecurity strategy that includes OJT as a key component, ensuring that training programs contribute to broader national security goals.
    - In summary, this strategic plan, emphasizes a balanced, wise, and just approach to enhancing OJT in cybersecurity. It recognizes the interconnectedness of individual development and national well-being, advocating for actions that benefit both students and the broader society.

Professional Development in Cybersecurity

Professional development in the field of cybersecurity can be significantly enhanced through practical learning experiences such as cyber competitions, hackathons, and similar activities. These events provide hands-on opportunities to apply theoretical knowledge, fostering the development of essential skills and competencies. Here is a brief list of significant components of such practical learning experiences:

1. **Technical Skills Development**: Participants engage in real-world scenarios requiring the application of technical skills such as penetration testing, network defense, ethical hacking, digital forensics, and incident response. This hands-on experience is invaluable for understanding the complexities of cybersecurity in practice.

2. **Problem-Solving**: Cyber competitions and hackathons present complex problems that require innovative solutions. Participants must think critically and creatively to identify vulnerabilities, mitigate risks, and secure systems, which enhances their problem-solving capabilities.

3. **Teamwork and Collaboration**: Many of these events are team-based, requiring participants to collaborate effectively. This fosters communication skills, leadership, and the ability to work under pressure, all of which are crucial in the cybersecurity field.

4. **Understanding of Real-World Threats**: Through simulations and challenges that mimic current cybersecurity threats, participants gain a deeper understanding of the landscape of cyber threats and the tactics, techniques, and procedures (TTPs) used by adversaries.

5. **Networking**: These events provide a platform for individuals to connect with peers, industry professionals, and organizations, facilitating the exchange of knowledge and opening up opportunities for mentorship, internships, and employment.

6. **Continuous Learning**: Cyber competitions and hackathons encourage continuous learning and skill development. They expose participants to the latest technologies, tools, and practices in cybersecurity, emphasizing the importance of staying updated in a rapidly evolving field.

7. **Ethical and Legal Considerations**: Participants learn to navigate the ethical and legal aspects of cybersecurity, understanding the importance of ethical hacking and the implications of cyber laws and regulations.

8. **Time Management and Prioritization**: Given the time-bound nature of these competitions, participants improve their ability to manage time effectively, prioritize tasks, and make quick, informed decisions.

Incorporating these components into professional development plans can significantly enhance an individual's preparedness for a career in cybersecurity, equipping them with the practical skills and competencies required to navigate the challenges of the field.

SECTION #9

AI Risks and Opportunities

Prepared By

Patrick Slattery, Director of Industry Engagement, Zicklin School, Baruch College, City University of New York (CUNY)

Background and Scope

In this section of the paper, the primary focus is on machine learning (ML) and deep learning (DL) techniques. These are subsets of artificial intelligence (AI), known for their ability to analyze large amounts of data, identify patterns, and make predictions or decisions with minimal human intervention.

Machine learning involves training algorithms on extensive datasets to recognize patterns and make decisions based on new data. This technique is crucial in enhancing cybersecurity measures by automating the detection of anomalies in network traffic, predicting potential security breaches, and responding to threats in real-time. These capabilities aid in developing adaptive cybersecurity defenses that can respond to evolving threats.

Deep learning, an advanced subset of machine learning, uses neural networks with many layers to model complex patterns and relationships within data. It is particularly effective in tasks requiring high-level abstraction and understanding, such as image and speech recognition and natural language processing. In cybersecurity, DL can identify sophisticated cyber-attacks like deepfakes, where technology creates realistic but fraudulent audio, video, or images for malicious use.

These AI techniques enable cybersecurity professionals to detect and address threats more efficiently and accurately than traditional methods. However, they also require a workforce skilled in data analysis, algorithm development, and ethical considerations to utilize their full potential responsibly and effectively.

AI Threats in Cybersecurity

AI's rapid advancements have significantly transformed the cybersecurity landscape. Major threats include enhanced and automated cyber-attacks, such as AI-driven phishing, malware, and ransomware. These advanced attacks exploit vulnerabilities more efficiently and on a larger scale than human attackers alone.

AI also boosts evasion techniques. Adversarial attacks and polymorphic malware use AI to create dynamic threats that evade standard security protocols and bypass traditional defenses.

Furthermore, AI has escalated data privacy concerns. Technology like deepfakes pose severe risks to personal and organizational privacy. AI-driven data harvesting and surveillance enable

intrusive and widespread data collection, often unbeknownst to the affected individuals, leading to potential reputational and financial damage.

AI Opportunities in Cybersecurity

Despite the threats, AI provides opportunities to enhance cybersecurity measures. It allows for enhanced threat detection and response in real time. Techniques like anomaly detection and predictive analytics enable proactive and effective security measures.

AI excels in automating security processes. It handles repetitive tasks, allowing human analysts to focus on more complex issues. AI streamlines operations and improves efficiency, ensuring swift and effective responses to potential threats.

Additionally, AI supports proactive cyber defense strategies. Predictive threat modeling and real-time monitoring anticipate and counteract threats before they happen, helping organizations stay ahead of attackers.

Workforce Requirements for AI-Driven Cybersecurity

AI integration into cybersecurity demands new skills and interdisciplinary expertise. Professionals must understand AI and machine learning principles and traditional cybersecurity knowledge. Essential skills include data analysis, algorithm development, and AI ethics understanding.

A holistic approach becomes necessary as the lines blur between cybersecurity, AI, data science, and ethics. Continuous learning and adaptation are vital in this rapidly evolving field.

Implications for Higher Education Offerings

Higher education institutions must adapt their curricula to address AI-driven cybersecurity. Integrating AI and cybersecurity into academic programs prepares future professionals. Courses like AI in Cybersecurity, Machine Learning, and Ethical Hacking offer foundational knowledge and practical skills.

Hands-on training and research opportunities are crucial. Practical experience bridges the gap between academic learning and practical application, developing problem-solving skills and a deep understanding of cybersecurity dynamics.

Collaboration with industry enhances higher education offerings. Partnerships provide students with access to cutting-edge technologies and real-world challenges, ensuring educational programs align with cybersecurity workforce needs.

In conclusion, AI's integration into cybersecurity presents significant threats and opportunities. Addressing these challenges requires a skilled and knowledgeable workforce, supported by higher education institutions that adapt their offerings to meet these evolving needs. By fostering interdisciplinary expertise, continuous learning, and practical experience, we can build

a resilient cybersecurity workforce to defend against AI-driven threats and leverage AI for enhanced security measures.

Conclusion

Effective and accessible cybersecurity professional preparation is one key to defending and protecting U.S. critical infrastructure, campus communities, organizations, and residents. A lacking comprehensive strategy and operational cybersecurity workforce development and education action plan jeopardizes many aspects of a democratic society. Nations with unchecked vulnerabilities fuel otherwise additional unmanaged risks down the road. Enhancing cybersecurity workforce capabilities and reducing capacity skill gaps is fundamental to bolster and reinforce current and future economic and national security. Securing K-12 and Higher Education campus digital infrastructure, networks, and data remains a pressing concern as well with a high frequency of cyberattacks and ransomware incidents at our schools, colleges, and universities. Cybersecurity workforce and education capability, infrastructure, capacity, and skills gaps are national security and economic issues of the highest order. However, there are significant structural issues and bottlenecks that limit the professional preparation, hiring, and retention processes. One purpose of this report was to describe essential factors and "best practices" to analyze and evaluate in the preparation of SME recommendations to enhance national cybersecurity K-12/Higher Education and Workforce Development.

Due to a significant learning curve related to cybersecurity workforce preparation and development, we remain behind this curve on finding and maintaining essential cybersecurity workforce supply and employer demand equilibrium. This demand for talent is found at all levels of the career ladder (entry-level, intermediate, and advanced work roles). To meet robust growth in the cybersecurity ecosystem, we need to counter this threat with cadres of future qualified and skilled cybersecurity professionals. These professionals are prepared through the operation of a national cybersecurity career education pipeline and pathway that simultaneously prepares workforce through traditional and non-traditional based approaches.

Cybersecurity career education pipelines/pathways must link, align, and network across all levels of K-12 Education and Higher Education. Cyber career pipeline are aligned with STEAM and CTE programs, courses, and content, and intended to reach across professional fields and academic disciplines. Pipelines/pathways rely on deep and meaningful collaborative partnerships with the public sector, private sector, academia, and CBOs. Cybersecurity pathways include both an academic and skills-based process to utilize the strength of each in the education, certifications, and workforce development model components. This pipeline/pathway links and aligns all levels of education with industry-based certifications and workforce development.

There are additional key components to study to better understand our progress and evaluation of the intricate and complex nexus found between cybersecurity education/training, workforce preparation, and reducing capacity-skills gaps. What are the next steps in effective cybersecurity workforce development and education? Given the growing convergence and impact of AI, cybersecurity, and tech, this uncertain future may not have been generated yet. A significant paradigm shift may indeed be in progress within the cybersecurity workplace.

References

Center for Strategic and International Studies (CSIS). "What to Make of the Newly Established CyberSecurity Association of China." CSIS, 25 May 2016, https://www.csis.org/analysis/what-make-newly-established-cybersecurity-association-china.

CISA. "Cybersecurity Workforce Development Resources." Cybersecurity > Education > Cybersecurity Workforce Development Resources, https://www.cisa.gov/cybersecurity-workforce-development-resources.

CISA. "Resources for Academia." Resources: Resources for Academia, https://www.cisa.gov/uscert/resources/academia.

CSAC. Cybersecurity Association of China (in Chinese). https://www.cybersac.cn/.

Dakota Cary. "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain." Center for Security and Emerging Technology, July 2021, https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center/.

George Sharkov. "Multi-Stakeholder Approach to Cybersecurity and Resilience." Academia.Edu, 2016, https://www.academia.edu/73196001/Multi_stakeholder_Approach_to_Cybersecurity_and_Resilience.

NIST. "Cybersecurity & Privacy Stakeholder Engagement." NIST.Gov, https://www.nist.gov/cybersecurity/cybersecurity-privacy-stakeholder-engagement.

NIST. "Stakeholders: The 'Be-All and End-All' of NIST's Cybersecurity and Privacy Work." NIST.Gov, 24 Mar. 2021, https://www.nist.gov/blogs/cybersecurity-insights/stakeholders-be-all-and-end-all-nists-cybersecurity-and-privacy-work.

Simone Fischer-Hübnera, Cristina Alcaraz, Afonso Ferreira, Carmen Fernandez-Gago, Javier Lopez, Evangelos Markatos, Lejla Islami, Mahdi Akila. "Stakeholder Perspectives and Requirements on Cybersecurity in Europe." Science Direct, Sept. 2021, https://www.sciencedirect.com/science/article/pii/S2214212621001381.

Additional References

https://www.isc2.org/research - global workforce student and women in cybersecurity

2018 study

https://www.zippia.com/cyber-security-analyst-jobs/demographics/ - U.S. Statistics

https://www.aspeninstitute.org/wp-content/uploads/2021/09/Diversity-Equity-and-

Inclusion-in-Cybersecurity_9.921.pdf - aspen institute

https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/Innovation-

Through-Inclusion-Report.pdf - 2018 ISC2 and Frost and Sullivan report

https://www.accenture.com/content/dam/accenture/final/capabilities/technology/security/

document/Accenture-Rising-to-the-Top-Accenture-Cybersecurity-Forum.pdf#zoom=50 -

2022, discusses the issue and why it is important

https://www.pewresearch.org/science/2021/04/01/stem-jobs-see-uneven-progress-in-increasing-gender-racial-and-ethnic-diversity/ - general stats for STEM fields 2017-2019

https://ncses.nsf.gov/pubs/nsf23315 - NSF STEM data 2022 (note women have the least percentage of math/computing degrees)

https://eric.ed.gov/?id=EJ895873 - 2010 Department of Education study on increasing minority participation in Computer Science

https://iacis.org/iis/2013/189_iis_2013_143-152.pdf - more background on the problem, 2013

https://www.cio.com/article/201905/women-in-tech-statistics-the-hard-truths-of-an-uphill-battle.html -

https://hbr.org/2016/11/why-diverse-teams-are-smarter

https://hbr.org/2023/10/the-conflict-resolution-skills-every-project-manager-needs

https://hbr.org/2017/03/teams-solve-problems-faster-when-theyre-more-cognitively-diverse