Broadening the search to narrow the gap:
This critical challenge project is intended to address the workforce shortage by evaluating the transformation that needs to occur including the evaluations of barriers to entry which disqualifies or overlooks candidates who are willing and capable of filling unfilled roles in cybersecurity. Specially, one organization is evaluated to determine what steps need to be taken to enhance and broaden an existing cybersecurity curriculum to best prepare students for a career in cybersecurity.

Abstract

With over 300,000 cybersecurity related jobs openings posted within the United States the past year, the inability to fill these roles exposes organizations to a greater level of cybersecurity risk. The shortage is exacerbated globally, where it's expected nearly three million cybersecurity jobs are expected to be unfilled.[1] Employers continue to seek individuals with previous cybersecurity experience even for entry-level roles, yet the lack of cybersecurity opportunities creates a significant barrier for many to enter the field and fill open roles. A progressive approach is necessary to fill these vacant cybersecurity roles, including looking at candidates who have previously been overlooked.

This report will primarily focus on how one organization, Year Up can serve as a model to bridge the cybersecurity workforce shortage by placing young adults in cybersecurity roles who would otherwise not have the opportunity. An analysis will be performed of the curriculum currently be taught in the San Francisco location to identify opportunities to update the curriculum to best prepare and market students for cybersecurity internships opportunities.

The next part of this report will evaluate how this program can expand to other Year Up locations within the United States. Currently, the cybersecurity curriculum is only offered at a handful of cities, limiting the number of Year Up students who are can enroll in the cybersecurity track. The lack of qualified instructors has resulted in a decentralized curriculum, resulting in inconsistencies in what is taught to students currently in the program.

[1] "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens." October 2018. Accessed January 2019. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0.

Last, an evaluation will be conducted to determine recommendations to be considered to increase engagement with corporate partners to increase the number of Year Up students who have cybersecurity internship opportunities.

Introduction

Cybersecurity has a people problem. It is well documented that people continue to be a weak link within the cybersecurity ecosystem, highlighted by the pervasiveness of attacks exploiting humans as a vulnerable attack vector. Nearly half of companies surveyed believed human error has led to data breach according to a 2018 survey of C-Suite and small business owners. [2] As cybersecurity practitioners work to improve training and awareness programs within their organizations, another people problem exists within the cybersecurity industry. Highlighted in the 2018 ISC[2] Cybersecurity Workforce Study, 59% of respondents noted their organization is at moderate or extreme risk due to their cybersecurity staff shortage. [3] Simply put, organizations with well-devised cybersecurity strategies are still at risk if the resources required are not available to execute the strategy. Figure 1 highlights how respondents from the workforce study believe their cybersecurity staffing levels are largely not meeting the needs to execute their cybersecurity programs.

[2] "Shred-it Study Exposes Employee Negligence | Shred-it | United States." Shred-it. June 20, 2018. Accessed January 3, 2019. https://www.shredit.com/en-us/about/press-room/press-releases/shred-it-study-exposes-employee-negligence.

[3] "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens." October 2018. Accessed January 2019. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0.

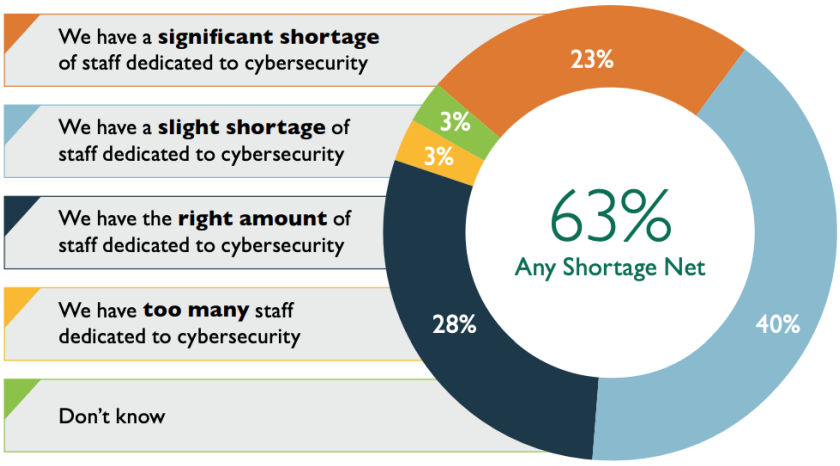

Figure 1 – Cybersecurity staff shortages[4]

These statistics reinforce the necessity to broaden the search for cybersecurity talent beyond the conventional method currently employed. Organizations seeking candidates should re-evaluate their hiring requirements which often include experience, education, and certification requirements for even junior level cybersecurity roles. Not each role placed in cybersecurity is a technical position, and organizations seeking resources should not recruit in a manner that suggests that technical skillsets are the only skills required. For example, an organization seeking a candidate to draft policies and standards, a strong writing background should be desired. For those responsible for training and awareness, understanding human behavior is an important attribute when creating an effective training program and awareness program for cybersecurity.

A review of the Bureau of Labor Statistics on the qualifications for an Information Security Analyst role includes, "most information security analyst positions require a bachelor's degree in a computer-related field. Employers usually prefer analysts to have experience in a related occupation". [5] This statement and specifically the requirements exemplify why the workforce shortage exists for cybersecurity in a very much self-inflected manner:

- The requirements for a bachelor's degree in a computer related field can often be accompanied by an additional requirement for having a master's degree.

[4] ibid
[5] "Summary." U.S. Bureau of Labor Statistics. March 09, 2018. Accessed june 17, 2018. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-4.

- Experience in related occupational is largely associated with having some level of information technology experience such as being a system administrator.

These requirements were identified by the Bureau of Labor Statistics for an information security analyst role, a position that many within cybersecurity will begin their career in. These requirements reflect and amplify a major misconception; cybersecurity is a technology issue requiring more technologist to solve. While technology and the advancements made will continue to play a central role in how the threat and risk landscape evolve and the defense mechanisms that are deployed, it homogenizes the skillsets that are seeking to address the cybersecurity workforce gap, and more broadly the cybersecurity challenge itself.

Apprenticeship programs have long existed to assist organizations in identifying and developing candidates to fill open roles within the organization. One organization who is a leader in leveraging this model is IBM, who has coined the term "new collar" to identify a workforce without a four-year degree but having developed the technical and soft skills to fill technology roles. IBM is betting on new collar works to the extent of a $1 billion-dollar investment to further develop this program. Not all organizations who have the same needs as IBM to fill these roles have the same level of resourcing to create an in-house program to develop the required technical and soft skills.

During my CCP flash presentation in June, I received a tremendous amount of feedback from the cohort on resources and organizations that I should look into partnering with to address the cybersecurity workforce shortage. One organization that particularly stood out was Year Up, an organization that focused on the opportunity divide with the mantra, *a hand up, not a handout*.

Year Up

Founded in 2000, Year Up is a not for profit that works with low to moderate income students, between the ages of 18-24, and without a four-year college degree. Year Up focuses on developing the individual in an intense one-year program that combines in-class learning, real-world experience, structured support, in a high expectation environment. The one-year program is divided into two six-month phases: learning & development and the internship phase.

Year Up has defined six core values it expects students to adhere to:

- Respect and value others.
- Build trust; be honest.
- Engage and embrace diversity.
- Be accountable.
- Strive to learn.
- Work hard and have fun.

To be admitted to the program, students are required to complete an online application as well as go through a series of interviews. When a student is admitted, they sign a contract that allows them to earn a weekly stipend which allows them to focus on being immersed in the program. The process to be admitted to the program maintains a high level of rigor as only one in six applicants are admitted to the program. Retention of admitted students is also high, where nearly 80% of students who enroll in the program end up completing the one-year program.

To uphold the Year Up values, each student in the program agrees to a contract that includes consequences that directly impact the stipend if infractions occur during their one-year tenure with the Year Up program. As captured in Table 1, students have expectations that when not met, results in a loss of points that correlate to dollars from their stipend. As such, the "high support, high expectation" model is established each of the Year Up campuses throughout the United States serving nearly 4,000 students.

Expectation	Description	Consequence of not meeting expectation
Arriving and leaving on time and notification of lateness	You are expected to be on time and prepared to start each class or activity at its scheduled start time and at the end of breaks. You are also expected to remain until the scheduled end time.	With notification: lose 15 points
		Without notification: lose 25 points

Regular attendance and notification of absences	You are expected to attend Year Up regularly. Proper is expected if you will not be attending. *Attending less than half the scheduled hours will be considered an absence.*	Absence with notification: no stipend, plus: Day 1-3 missed days: Leave days Day 4-6 missed days: lose 25 points Day 7-9 missed days: lose 35 points Over 10 days missed: lose 45 points
		Absence without notification: no stipend, plus: Day 1-6 missed days: lose 50 points Day 7-9 missed days: lose 60 points Over 10 days missed: lose 70 points
Business dress	You are expected to wear business attire during all activities at Year Up.	Lose 15 points
Appropriate use of Year Up computers	You are expected to follow the Computer Acceptable Use Policy	Lose 15 points
Appropriate use of electronic devices	You are expected to use your cell phone and other electronic devices appropriately	Lose 15 points
Complete assignments on time	You are expected to turn in all assignments for classes by the due date, unless other arrangements have been made in advance with the instructor.	Lose 15 points
Attend all planned meetings	When you have a scheduled meeting, you are expected to honor the commitment. If unable, due to circumstances beyond your control, you should make alternate arrangements in advance with the other individual(s) involved.	Lose 15 points
Follow site norms / policies and procedures of site norms	When you are on the site, you are expected to follow the procedures for the site.	Lose 15 points and will be recorded as a core value infraction
Respect the law		

	At Year Up, you are expected to avoid engaging in theft, vandalism, sexual harassment, drug/alcohol possession or use, weapon possession, fighting, piracy, and other illegal activities.	At the discretion of the Year Up staff, penalties up to and including being fired from the program.
Respect the core values of Year Up	In addition to the expectations above, you are expected to behave in a manner consistent with the core values of Year Up.	At the discretion of the Year Up staff, loss of 15, 25, or 50 points.
Demonstrate internship readiness	You are expected to earn C's or higher in all courses and to pass the internship readiness assessment.	At the discretion of the Year Up Staff, penalties for not passing the Internship Readiness Assessment or passing all classes is being fired from the program.

Table 1 – Year Up Student Contract

After completion of the learning and developing phase, students are placed in internships with corporate partners. These corporate partners make span multiple industries, often times in a Fortune 500 organization (including Brown University). Students spend four-and-a-half days a week at their internship before returning for half a day each week to continue on-campus learning and development. Feedback is a critical component of the program, where students continuously are provided constructive feedback to foster their development from both internship partners and Year Up staff.

The results of the Year Up are quantifiably positive. Nearly all (99%) of students that start the learning & development phase of the program end up completing that portion of the program. 91% of graduates are either employed or enrolled in post-secondary education within four months of graduation. Those who enter the workforce make an average of $19 an hour, equating to a salary of nearly $40,000 annually.[6] From the corporate partnership perspective, over 90% are satisfied with the program and would recommend the program to their peers and colleagues. [7]

[6] "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens." October 2018. Accessed January 2019. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0.

[7] "2017 Year Up Annual Report." 2018. Accessed October 22, 2018. https://www.yearup.org/wp-content/uploads/2018/05/2017-Year-Up-Annual-Report.pdf.

The Cybersecurity Track

After being provided contact information for Year Up, a meeting was scheduled with the Program Manager of Year Up Silicon Valley to better understand if cybersecurity was part of the existing program. During this initial conversation, it was noted a cybersecurity track existed and was first developed for the San Francisco location as a pilot program in 2015. The program has since expanded to other Year Up locations including Boston, Chicago, Atlanta, and Baltimore and currently includes 70 students and 280 alumni.

Very little documentation exists from Year Up on the cybersecurity track. A search on their website yields little results to conclude that cybersecurity exists in the program. A broader search online points to a partnership with Symantec Corporation to introduce students to cybersecurity. When asked for an overview of the cybersecurity program from the Program Manager, the following description was provided:

Cyber Security - *The course is designed to describe the impact of cyber security in the United States and globally; identify threats to network services, devices, traffic, and data; identify the features and techniques needed to secure network communications; describe a PKI (Public Key Infrastructure) and explain how a PKI scheme is managed; identify the elements that make up an organizational security policy, and describe the measures needed to enforce it; describe how a security infrastructure is monitored; and describe risk management and identify network monitoring tools that help support it.*

In reviewing the description of the course, while it touches upon important aspects of cybersecurity including the impacts domestically and globally, the role of technology, and the importance of policies, there are critical components related to cybersecurity that are not covered.

In September 2018, a meeting with the Academic Director of Year Up Bay Area who contributed to developing the cybersecurity course was conducted to understand how the course was constructed. It was acknowledged that the cybersecurity course did not consider cybersecurity more broadly – including how to include non-technical components to the curriculum. Another item that was noted during the conversation was the curriculum for cybersecurity was not consistently developed and rolled out to each

location currently offering the cybersecurity track. A student in the cybersecurity track in San Francisco is currently being taught different content than a student in the Boston and other Year Up locations. As such, no singular curriculum can be evaluated for this analysis, rather using the curriculum in San Francisco for the more in-depth analysis below.

Cybersecurity Curriculum Analysis

LAMP Stack and Scripting

The cybersecurity track at Year Up San Francisco consists of two seven-week modules that students complete as part of the learning and development phase. The first seven weeks are focused on LAMP stack and scripting languages to familiarize students with open source web architecture and the scripting languages used to develop them. As captured in Figure 2, students take two classes a day Monday through Thursday, with one class on Friday. Assignments and quizzes are given to reinforce student engagement and understanding of the topic being discussed for the day. As noted in Table 1, students are expected to maintain a C's or higher, so engagement is required prior to getting to the internship phase of the program.

Major Topic(s)		Monday	Tuesday	Wednesday	Thursday	Friday
Week 9						
LAMP Stack	Content/Practice	OSI and Network Protocols	CentOS Minimal Install with	Linux Network	Linux Super Users and	
	Assignment	Project - Troubleshooting Your	Deliverable - Introduction to	Deliverable - Clone Wars	Deliverable - SSH and	
	Assignment Due	Deliverable - Apache Server	Deliverable - The OSI Model	Deliverable - Linux: Web		Project - Troubleshooting
	Quiz	Exit Ticket - Sausage Pizza	Exit Ticket - VI and You	Exit Ticket - SSH Image		
	Performance				Formative Assessment -	
CIS 303 Scripting Languages	Content/Practice	IF ELSE Statements and Logic	While and For Loops		Switch Statements	
	Assignment	Deliverable - Pronouns	Deliverable - Counting		Deliverable - Personal	
	Assignment Due	Deliverable - LinkedIn Learning,	Deliverable - Pronouns	Deliverable - Counting		Week 09 Status Report
	Quiz	Exit Ticket - Choices	Exit Ticket - Random		Exit Ticket - Too Many	
	Performance					Formative Assessment

Figure 2 – Sample Weekly Schedule

In reviewing an extract of the topics covered for the LAMP stack and scripting languages which is captured in Table 2, there are a handful of questions that are important to consider when evaluating the content within each module. The first question is to what extent is this content relevant to the internship opportunities the students in the cybersecurity track will obtain? It is also important to be pragmatic during the evaluation period that no curriculum can be developed to fully prepare students for the internships that they will embark on – especially in a six-month program.

LAMP Stack	Scripting Languages
MacBook Administration, VirtualBox with Linux Distributions	GitHub and UNIX/Linux permissions
VirtualBox with Linux Distributions	Variables and System Variables
CentOS 7 GUI Server Install	The Different Quotation Marks
Linux Commands, STDIN, STDOUT, STDERR	IF ELSE Statements and Logic Tests
OSI and Network Protocols	While and For Loops
CentOS Minimal Install with VI Text Editor	Switch Statements
Linux Network Configurations and SSH	Arrays
Linux Super Users and Ports	Arrays inside Arrays and Switches
IPv4 Subnetting	Functions
Routing and Switching	HTML, CSS Review
DHCP & NAT, Ports and Packets	Introduction to JavaScript
ROAS and Layer 2 and VLANs	The Document Object
TCP Flags with WireShark	Debugging with Browser Development Tools
MySQL and Relational Databases	Console Breaks
PHP	Introduction to jQuery
	jQuery for HTML Output
	Application Program Interface

Table 2: Technical Module Topics

In reviewing the content covered in both LAMP stack and scripting language, the role in cybersecurity that is best suited for the content is within product security. Product security has evolved from security as an add-on during initial product release, to a program to continuously improve the security posture of the application to keep pace with the evolving vulnerability and threat landscape.[8]

[8] Covington, Robert C., and Robert C. Covington. "Product Security: Not Just Bells and Whistles." CSO Online. October 19, 2016. Accessed January 24, 2019. https://www.csoonline.com/article/3131614/internet-of-things/product-security-not-just-bells-and-whistles.html.

Additionally, to compare the LAMP stack and scripting language module to filled internship opportunities, a list of internships that students within the cybersecurity track have filled in San Francisco was obtained and captured below in Table 3. The wide range of internships further solidifies the importance of a diverse curriculum for students and that the focus on LAMP stack and scripting language may only benefit a handful of the internship opportunities including Cloud Security Engineer Intern, Pen Testing Intern, and Security Systems Interns.

San Francisco Cybersecurity Internship Opportunities	
Cloud Security Engineer Intern	Cyber Analyst
Cyber Compliance Research Intern	Cyber Engineering Intern
Cyber Security Analyst	Cyber Security Intern
Cyber Security PMO Program Consultant	Detection & Monitoring Operations (D&MO) Intern
Digital Certificate & Encryption Automation Intern	End User Computing Intern
Global Operations & Security Intern	Identity & Access Management Intern
Information/Network Security Intern	Information Security Intern
INFOSEC Security Analyst	ISPO Intern (Info. Sec. and Privacy Intern)
IT Cyber Threat Intelligence Analyst	IT Network Specialist
IT Risk and Security Intern	Security Intern
Jr. Cyber Analyst	Jr. Risk Analyst - Trust and Assurance Group
Pen Testing Intern	Security Awareness Intern
Security Operations Intern	Security Systems Intern
SOC Analyst intern	Strategy and Incident Intern
Technology Risk Security Analyst	Technology Services - Cloud Engineer
Third Party Trust Intern	Vulnerability Analyst Intern

Table 3: Cybersecurity Internships

Students have little influence on which internship they are placed in during as part of the program, which further emphasizes that necessity for a balanced overview of cybersecurity during the learning & development phase of their Year Up experience. Additionally, given that students will potentially gravitate towards more specific domains within cybersecurity, consideration needs to include which role best suits each student success and full-time placement perspective prior to assignment of internships.

Cybersecurity

The final seven weeks of the learning & development phase are focused on other cybersecurity topics, referred to as module 3. As captured in Table 4, the topics lean heavily towards the computer security topics within cybersecurity. In those seven weeks, students will be exposed to topics including how encryption can protect the confidentiality of information, and how attackers use readily available tools to perform attacks. Labs provide students hands-on experience on how to prevent cybersecurity

attacks by going through the cyber kill chain. Quizzes are given to reinforce key takeaways from each topic area.

Cybersecurity
Kali Linux & Microsoft Appliance Installation and Overview
Confidentiality, Integrity, Availability & Authentication, Authorization
Cyber Security Kill Chain
Password Hashes
Synchronous and Asynchronous Encryption
RSA Encryption and Private and Public Keys
Wireless Exploits with Airodump-ng
Man in the Middle Attack with AC 1200 Wireless Adapter
Governance, Risk, and Compliance
ISO 27001
NIST Cybersecurity

Table 4: Cybersecurity Module Topics

To evaluate the existing curriculum against a generally accepted security framework, the NIST Cybersecurity Framework was selected to evaluate the existing curriculum against. The categories and sub-categories captured in Figure 2 were mapped to the topics that are currently included module 3 of the cybersecurity track. Table 5 captures the mapping (with corresponding colors) that was conducted at both the category and sub-category level of the NIST Cybersecurity Framework.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

***Figure 2 – NIST Cybersecurity Framework*[9]**

[9] Ausherman, Nicole. "MEP Centers Aid Manufacturers on Cybersecurity." NIST. May 03, 2018. Accessed December 24, 2018. https://www.nist.gov/news-events/news/2018/05/mep-centers-aid-manufacturers-cybersecurity.

Cybersecurity	NIST Cybersecurity Category or Subcategory
Kali Linux & Microsoft Appliance Installation and Overview	**Not applicable**
Confidentiality, Integrity, Availability & Authentication, Authorization	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Cyber Security Kill Chain	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
Password Hashes	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
Synchronous and Asynchronous Encryption RSA Encryption and Private and Public Keys	PR.DS-1: Data-at-rest is protected PR.DS-2: Data-in-transit is protected
Wireless Exploits with Airodump-ng Man in the Middle Attack with AC 1200 Wireless Adapter	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Governance, Risk, and Compliance ISO 27001 NIST Cybersecurity	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Table 5: Module 3 to NIST Cybersecurity mapping

Given the comprehensiveness nature of the NIST Cybersecurity Framework, it is unrealistic to expect a seven-week program to cover all categories. However, it is valid to argue that each of the higher level five functions of the NIST Cybersecurity framework should be included in a more thorough review as part of module 3 of the cybersecurity track. Specifically, none of the categories within the Respond or Recovery functions are included within the current curriculum. These functions are critically important under an "assume breach" scenario, where organizations are focused on detection, response, and recovery capabilities. Organizations that can timely respond to a breach (including containment) with an incident response team have been shown the ability to manage overall breach cost, as reported in 2018 IBM breach study. [10] These statistics will drive organizations to fill roles to bolster incident response capabilities, as shown by the 6,605 roles listed as available via CyberSeek in Figure 3.

[10] "IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses." IBM News Room. July 11, 2018. Accessed October 24, 2018. https://newsroom.ibm.com/2018-07-11-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US&cm_mc_uid=0328317361271546726992 3&cm_mc_sid_50200000=77975441548295404739&cm_mc_sid_52640000=55419241548295404761.

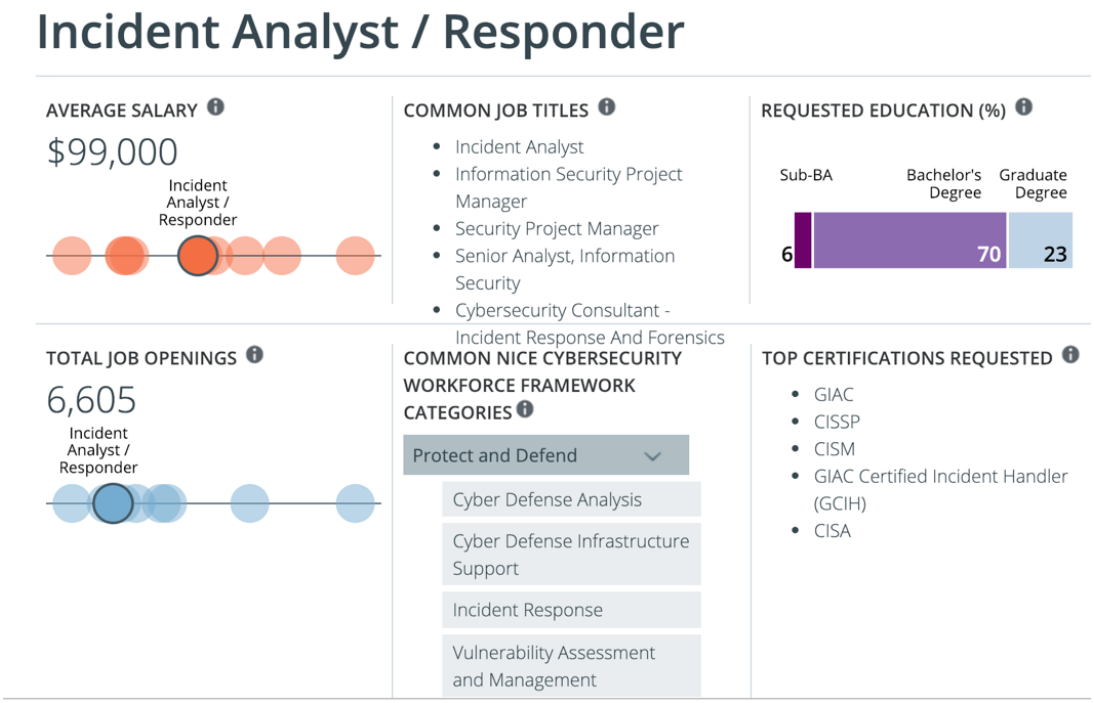

Figure 3 – CyberSeek Incident Response Roles[11]

Even under functions within the NIST Cybersecurity Framework that are currently covered in module 3, the topics only address a handful of the sub-categories within the NIST framework. For example, under the Identify function of the NIST framework, students are only lightly exposed to governance, risk management, and risk management strategies. Another example existing within the Detection function where students are not exposed to the human factor of cybersecurity, and how training and awareness programs can manage people risk from a cybersecurity perspective. As such, leveraging a generally accepted framework is one mechanism that Year Up can utilize to evaluate the robustness of their currently cybersecurity curriculum.

Beyond security frameworks, another perspective to evaluate the curriculum is how to best increase the marketability of the students as they first enter the internship phase, and hopefully either pursue higher education or full-time employment upon completion of their internship. Certificates and certifications are one mechanism that individuals can demonstrate their proficiency in cybersecurity. “Starter” level certificates and certifications are available within cybersecurity including ISACA’s CSX, CompTIA

11 "Cybersecurity Career Pathway." Cyberseek. Accessed June 24, 2018. https://www.cyberseek.org/pathway.html.

Security+, and ISC[2] Systems Security Certified Practitioner (SSCP).[12] Of these certifications and certifications, the CSX Fundamentals Certificate from ISACA does not require previous work experience or have minimum educational requirements, making it an achievable certificate for those within the Year Up cybersecurity track.

ISACA's Cybersecurity Fundamentals certificate is the first of three CSX certificates offered by ISACA. The CSX series of certificates were first introduced in 2015 and supplement other certifications offered by the organization. The Cybersecurity Fundamentals certificate markets itself towards three groups of future cybersecurity practitioners[13]:

- Professionals looking for a career change into cybersecurity
- Recent college graduates
- Others who are interested in cybersecurity

The exam covers five domains in which 75 questions within the domains covered in Figure 4. Those who are seeking the certificate must achieve a minimum passing score of 65% or higher.

[12] Lindros, Kim. "5 Great 'Starter' Cybersecurity Certifications." Business News Daily. December 28, 2016. Accessed January 2, 2019. https://www.businessnewsdaily.com/9661-cybersecurity-certifications.html.

[13] "ISACA Cybersecurity Fundamentals." August 2016. Accessed January 3, 2019. http://www.isaca.org/cyber/Documents/CSX-Fundamentals-Brochure-with-pricing_Bro_Eng_0816.pdf.

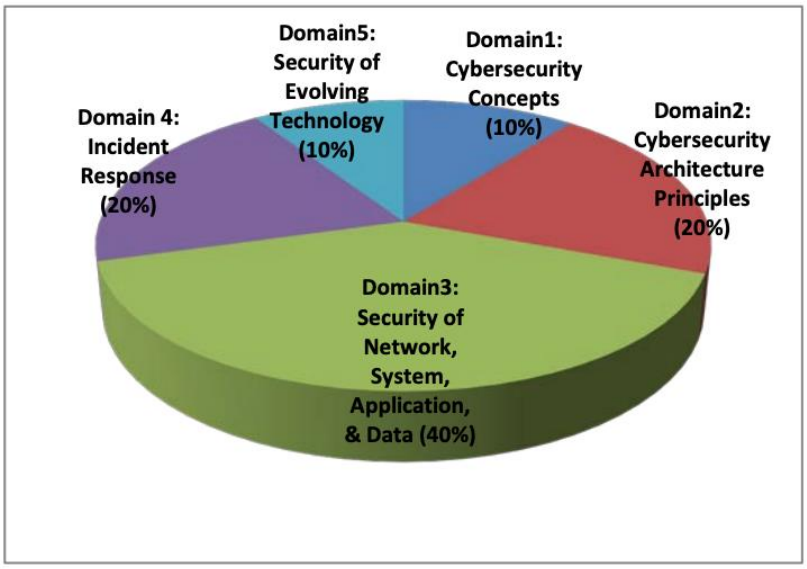

Figure 4 – ISACA CSX Fundamentals Exam[14]

An analysis of the five domains of this exam identifies overlap with the NIST Cybersecurity Framework; many of the same topics that are currently not included within module 3 of the cybersecurity track. One difference is the ISACA content has collapsed disaster recovery and business continuity into Domain 4 with incident response, while the NIST Cybersecurity Framework includes them within the Recover function. There are topics within the NIST Cybersecurity Framework that are not included in the CSX Fundamentals content in Table 6. Two notable areas that are not included as topic areas are asset management and training and awareness within the CSX Fundamentals.

[14] ibid

Domain1: Cybersecurity Concepts
Risk
Common Attack Types and Vectors
Policies
Cybersecurity Controls

Domain 2: Security Architecture Principles
Overview of Security Architecture
The OSI Model
Defense in Depth
Information Flow Control
Isolation and Segmentation
Logging, Monitoring, Detection
Encryption Fundamentals

Domain 3: Security of Networks, Systems, Applications and Data
Process Controls—Risk Assessments
Process Controls—Vulnerability Management
Process Controls—Penetration Testing
Network Security
Operating System Security
Application Security
Data Security

Domain 4: Incident Response
Event vs. Incident
Security Incident Response
Investigations, Legal Holds and Preservation
Forensics
Disaster Recovery and Business Continuity

Domain 5: Security of Evolving Technology
Current Threat Landscape
Advanced Persistent Threats
Mobile Technology
Consumerization of IT and Mobile Devices
Cloud and Digital Collaboration

Table 6: ISACA CSX Fundamentals Topics

The Program Manager in San Francisco has the authority to change the content in each module as needed. This was evident when feedback was provided on compliance and regulatory frameworks to be included in the curriculum. It's also important to reiterate that this curriculum is specific to San Francisco location, and other Year Up locations are likely to have a different content within their cybersecurity track. This creates challenges not only in maintaining a curriculum that delivers relevant and quality content, but it also creates a challenge to being able to scale the cybersecurity to other Year Up locations.

It is recommended that Year Up create one curriculum for all locations offering the cybersecurity track. Developing one curriculum allows Year Up to maintain the delivery of high quality and relevant content to students, regardless of location. The content should focus on providing students with a broad overview of cybersecurity, while preparing them to take and pass the ISACA CSX Fundamentals Certificate exam.

Including an industry recognized certificate is critically important to build the credibility and marketability of graduates of the program. As one of the few certificates in cybersecurity that does not require previous work experience, Year Up students can immediately obtain the certificate after the learning & development or during their internship phase. As they develop experience within cybersecurity, they can work to obtain higher level CSX certifications including the CSX Technical Foundation Certificates, CSX Practitioners, or Certified Information Security Manager (CISM). Alternatively, students can look to obtain certifications from other organization including ISC^2 Certified Information Systems Security Professional (CISSP).

Cybersecurity Track Expansion

The Year Up Cybersecurity track is not currently available at all Year Up Campuses nationwide mapped in Figure 5. One of the primary reasons is the lack of qualified instructors to teach and facilitate the cybersecurity curriculum. Per conversation with the Academic Director of Year Up, it was noted that Year Up struggles to compete against organizations that are seeking the same qualified candidate to fill many of the unfilled roles in cybersecurity to expand the cybersecurity track.

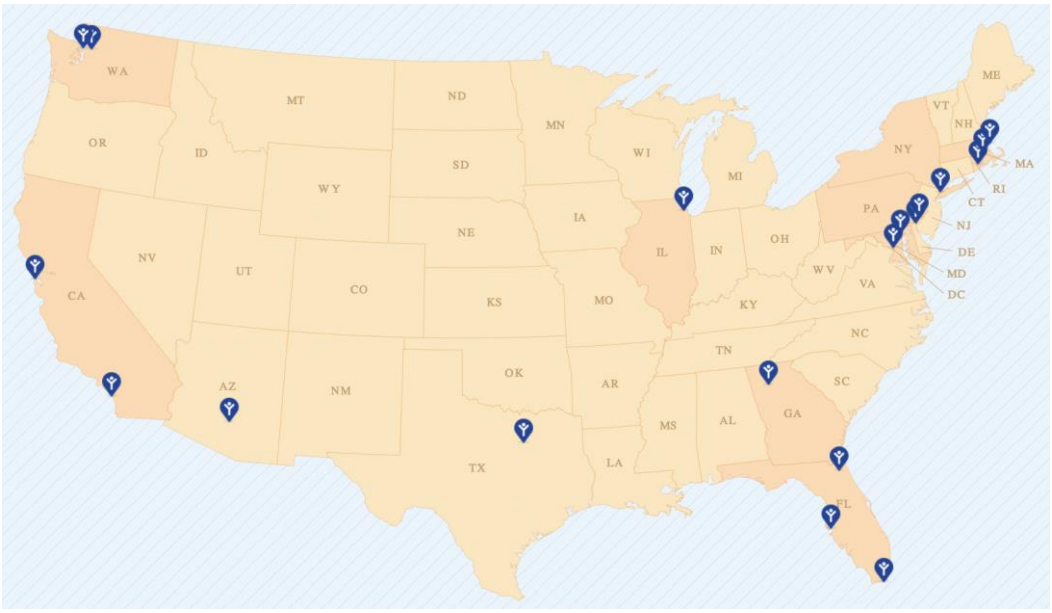

Figure 5 – Year Up Location[15]

15 "Our Locations." Year Up. Accessed June 24, 2018. https://www.yearup.org/about-us/our-locations/.

When evaluating where cybersecurity roles are available via CyberSeek, a tool provided by the National Institute of Cybersecurity Education (NICE), there is a strong correlation with the Year Up locations. As captured in Figure 6, many of the open roles are located where Year Up campuses exist, furthering the argument of expansion of the cybersecurity track to other campuses. This is not a complete coincidence as Year Up targets urban campuses to attract students from low to moderate income areas, with sufficient corporate partners to place students in internships at the completion of the learning & development phase.

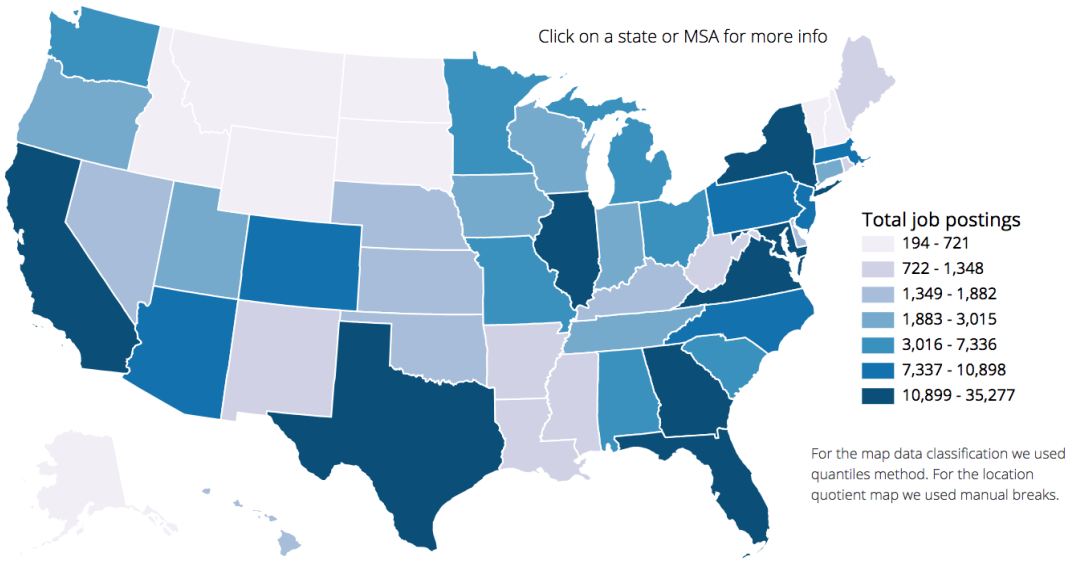

Figure 6 – CyberSeek Job Heatmap[16]

Currently, campuses that are unable to employ an instructor must rely on the cybersecurity track to be taught at local community colleges. This exacerbates the challenge of maintaining and delivering a consistent curriculum as the instructors at the local community colleges have the autonomy to teach content as they deem appropriate. While this method potentially provides one avenue of expansion of the cybersecurity track to other Year Up campuses, without a consistent curriculum, no consistent messaging can centrally be communicated as to how Year Up prepares students for cybersecurity internships and other future roles.

16 "Cyber National Level." Cyberseek. Accessed January 13, 2019. https://www.cyberseek.org/heatmap.html.

Building upon the recommendations made within the evaluation of the curriculum of the cybersecurity track, the content of the curriculum must be centrally managed and distributed to all locations offering the cybersecurity track. A committee of individuals representing the various campus locations should be formed along with those from the Year Up corporate office to manage the content for the cybersecurity track for all locations. Corporate partners can also be engaged to provide another perspective on what skill set or knowledge they observe as requiring to be developed as the cybersecurity track looks to expand and mature.

In addition to providing feedback on the cybersecurity curriculum, corporate partner engagement can extend into participating in the Year Up classroom. Guest instruction was a teaching method that I worked with the Program Manager to pilot for the San Francisco cybersecurity track. This would require approximately one-and-a-half hours of in-class instruction which included lecturing and engaging students through examples and questions and answers. If content needs to be created include lecture material, labs, and quizzes, this can significantly increase the time commitment from the guest instructor. It is advised that this content is provided as discussed above to be mindful of the level of hours required to be committed while creating incentives from a recruiting perspective for those corporate partners who volunteer their resources to participate. This experience allows for direct engagement with cybersecurity student and allows for participating individuals to gauge potential capability and fit for internship opportunities.

With the structure of the Year Up program and the support mechanisms that are in place to maintain a high engagement level from each student, remote or online learning has not been a tool that has been previously utilized. Per observation of three sessions within module 3 of the cybersecurity track, students are expected to engage heavily with one another, including a daily “warm-up” session in which students are each expected to respond to a question. As such, until technology can be supported within each location to allow live, interactive sessions, remote or online learning will be unlikely in any capacity as part of the cybersecurity track.

Corporate Engagement

As previously noted, there is little content available online for the Year Up and the cybersecurity program – both from a student and corporate partner perspective. A Google search yields only a handful of results, including videos from students who were part of the original program in 2015. As such, prospective students cannot confirm that the cybersecurity track is available at Year Up, and what potential internships the cybersecurity track can prepare them for. Corporate partners who are seeking cybersecurity interns cannot do so unless they have existing relationships and contacts at Year Up or through word of mouth. As such, prospective corporate partners do not have an accessible source of information, likely leading them to other sources to fill their cybersecurity roles. An awareness effort is required beginning with including greater content on the Year Up website to promote and attract both prospective students and corporate partners.

Using the CyberSeek data as a starting point, Year Up should gather information with their corporate partners in cities where cybersecurity roles are unfilled. If there are roles that can be filled by interns within the cybersecurity track, Year Up should collect this data to determine how to both prepare and market the cybersecurity track as a source of untapped source of future cybersecurity talent in those cities. One unique offering that Year Up provides is its *Custom Solutions* partnerships, where a program is designed and tailored for a specific corporate partner based on corporate partner needs. Corporate partners who have many roles or the need for a pipeline of talent can work with Year Up to develop specific content to be taught to best prepare the students for a role within the partnering organization. Based on CyberSeek data, a Custom Solution can be tailored to train students in a particular discipline in cybersecurity such as working on an incident response team, if that need exist more broadly in a city.

As discussed with various Year Up staff within the San Francisco Year Up office, the stigma that students need four-year degrees for entry-level roles still continues to be one of the significant barriers that students of year Up must face while seeking employment. With historic lows in unemployment, there has been a shift in hiring practices from emphasizing college degrees to a greater emphasis on skills needed to be successful in a role. Only 35% of employers believed that students were well prepared with both technical and soft skills to perform at a high level based on a study

performed by Bloomberg and Workday.[17] Notable organizations have altered their hiring requirements including Google, Apple, and EY. The intent is not only to address the workforce gap but increase diversity by including those who may have seen the cost of a four-year degree as a barrier to pursuing a career in a field of interest.[18] This is a significant opportunity for Year Up to increase corporate engagement by identifying organizations who have shifted hiring practices. Year Up students present a prime candidate pool to fill these roles based on the aforementioned trends in hiring and the emphasis in skills – both technical and soft. Proactive outreach will be critical by Year Up to position these students for cybersecurity opportunities for existing and especially those who do not yet partner with the organization.

Conclusion

One organization cannot address the cybersecurity workforce shortage, yet it can serve as a model to introduce those who have previously been overlooked and provide the opportunity needed. Year Up has developed a model long before cybersecurity workforce needs were identified by providing a "hand up and not a handout" to students. These students who largely come from lower income and diverse backgrounds have proven that when given the structure of a high support and expectation environment, they are able to thrive. Corporate partners echo the same sentiment based on level recurring engagement and willingness to recommend the Year Up program to others at a rate of 90%.

The cybersecurity track at Year Up has already provided students with a bevy of internship opportunities. These internship opportunities range from policy to technical roles which require students to have a well-rounded learning and development phase prior to their internships. While evaluating the curriculum for the San Francisco cybersecurity track, while critical foundation topics are covered, there are key topics including responding to incidents or disaster recovery that can be critical to include to

[17] Inc. "Workday and Bloomberg Next Study Reveals Need for Greater Collaboration Between Academia and Business to Close the Skills Gap." GlobeNewswire Newsroom. June 28, 2018. Accessed January 13, 2019. https://globenewswire.com/news-release/2018/06/28/1531112/0/en/Workday-and-Bloomberg-Next-Study-Reveals-Need-for-Greater-Collaboration-Between-Academia-and-Business-to-Close-the-Skills-Gap.html.

[18] Florentine, Sharon, and Sharon Florentine. "More Tech Companies Drop College Degree Requirement." CIO. September 28, 2018. Accessed February 1, 2019. https://www.cio.com/article/3309059/careers-staffing/more-tech-companies-drop-college-degree-requirement.html.

provide students a robust view of cybersecurity. A decentralized curriculum creates consistently challenges with both cybersecurity content and quality of material that will need to be evaluated as Year Up seeks to expand the cybersecurity track to other cities. To further increase the marketability of the students who graduate from the cybersecurity track, opportunities should be evaluated to align the curriculum to prepare students to obtain professional certificates to bolster their appeal to corporate partners and other organizations seeking cybersecurity talent.

The alignment in a consistent curriculum across multiple campuses is critical to both communicating at a national level what corporate partners and other organizations can expect from a Year Up cybersecurity graduate. Additionally, a centrally managed curriculum can reduce the need for reliance on local community colleges to teach a different curriculum, while reducing the burden for those who may be interested in volunteering their time to teach. Those corporate partners who volunteer their time to both curriculum buildout and in-class instruction should be incentivized for their participation with priority in recruiting for sought after cybersecurity resources.

While the stigma will continue to exist, the trend of shifting away from a four-year college degree as a necessity to be qualified continues to gain momentum. With notable employers adjusting their hiring requirements, Year Up is in prime position to reach out to both existing corporate partners and other organizations to actively market the success of their students as a prized pool of a talented workforce that historically has been untapped. While the most critical factor in the long-term viability of the cybersecurity track remains with the students and their performance within corporate partner organizations, Year Up should actively work with these corporate partners to provide these students with the best path to success. This success not only translates to the long-term viability of the cybersecurity track but is critical in serving as that model that can be leverage elsewhere so others who do not have the opportunity can fill the void that the cybersecurity desperately needs.

Bibliography

[1] "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens." October 2018. Accessed January 2019. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0.

[2] "Shred-it Study Exposes Employee Negligence | Shred-it | United States." Shred-it. June 20, 2018. Accessed January 3, 2019. https://www.shredit.com/en-us/about/press-room/press-releases/shred-it-study-exposes-employee-negligence.

[3] "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens." October 2018. Accessed January 2019. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0.

[4] ibid

[5] "Summary." U.S. Bureau of Labor Statistics. March 09, 2018. Accessed June 17, 2018. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-4.

[6] "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens." October 2018. Accessed January 2019. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0.

[7] "2017 Year Up Annual Report." 2018. Accessed October 22, 2018. https://www.yearup.org/wp-content/uploads/2018/05/2017-Year-Up-Annual-Report.pdf.

[8] Covington, Robert C., and Robert C. Covington. "Product Security: Not Just Bells and Whistles." CSO Online. October 19, 2016. Accessed January 24, 2019. https://www.csoonline.com/article/3131614/internet-of-things/product-security-not-just-bells-and-whistles.html.

[9] Ausherman, Nicole. "MEP Centers Aid Manufacturers on Cybersecurity." NIST. May 03, 2018. Accessed December 24, 2018. https://www.nist.gov/news-events/news/2018/05/mep-centers-aid-manufacturers-cybersecurity.

[10] "IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses." IBM News Room. July 11, 2018. Accessed October 24, 2018. https://newsroom.ibm.com/2018-07-11-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US&cm_mc_uid=03283173612715467269923&cm_mc_sid_50200000=77975441548295404739&cm_mc_sid_52640000=55419241548295404761.

[11] "Cybersecurity Career Pathway." Cyberseek. Accessed June 24, 2018. https://www.cyberseek.org/pathway.html.

[12] Lindros, Kim. "5 Great 'Starter' Cybersecurity Certifications." Business News Daily. December 28, 2016. Accessed January 2, 2019. https://www.businessnewsdaily.com/9661-cybersecurity-certifications.html.

[13] "ISACA Cybersecurity Fundamentals." August 2016. Accessed January 3, 2019. http://www.isaca.org/cyber/Documents/CSX-Fundamentals-Brochure-with-pricing_Bro_Eng_0816.pdf.

[14] ibid

[15] "Our Locations." Year Up. Accessed June 24, 2018. https://www.yearup.org/about-us/our-locations/.

[16] "Cyber National Level." Cyberseek. Accessed January 13, 2019. https://www.cyberseek.org/heatmap.html.

[17] Inc. "Workday and Bloomberg Next Study Reveals Need for Greater Collaboration Between Academia and Business to Close the Skills Gap." GlobeNewswire News Room. June 28, 2018. Accessed January 13, 2019.

https://globenewswire.com/news-release/2018/06/28/1531112/0/en/Workday-and-Bloomberg-Next-Study-Reveals-Need-for-Greater-Collaboration-Between-Academia-and-Business-to-Close-the-Skills-Gap.html.

[18] Florentine, Sharon, and Sharon Florentine. "More Tech Companies Drop College Degree Requirement." CIO. September 28, 2018. Accessed February 1, 2019. https://www.cio.com/article/3309059/careers-staffing/more-tech-companies-drop-college-degree-requirement.html.