Journal of Cybersecurity Education, Research and Practice

Volume 2022 | Number 2 Article 7

January 2023

Reinventing Cybersecurity Internships During the COVID-19 Pandemic

Lori L. Sussman
University of Southern Maine, lori.sussman@maine.edu

Reinventing Cybersecurity Internships During the COVID-19 Pandemic

Abstract

The Cybersecurity Ambassador Program provides professional skills training for emerging cybersecurity professionals remotely. The goal is to reach out to underrepresented populations who may use Federal Work-Study (FWS) or grant sponsored internships to participate. Cybersecurity Ambassadors (CAs) develop skills that will serve them well as cybersecurity workers prepared to do research, lead multidisciplinary, technical teams, and educate stakeholders and community members. CAP also reinforces leadership skills so that the next generation of cybersecurity professionals becomes a sustainable source of management talent for the program and profession. The remote curriculum innovatively builds non-technical professional skills (communications, teamwork, leadership) for cybersecurity research through student-led applied research and creating community-focused workshops. These student-produced workshops are in phishing, identity and privacy cyber safety, social media safety, and everyday home cyber safety. The CAs tailor the program to a particularly vulnerable population such as older adults, students, veterans, or similar people that make up most workshop participants. At this time, the data shows that this pedagogical approach to curriculum development, grounded in the Ground Truth Expertise Development Model (GTEDM), is a unique methodology. This curriculum teaches cybersecurity interns with key non-technical but critical KSAs for cybersecurity professional development has proved to be a factor in accelerated hiring for program participants.

Keywords

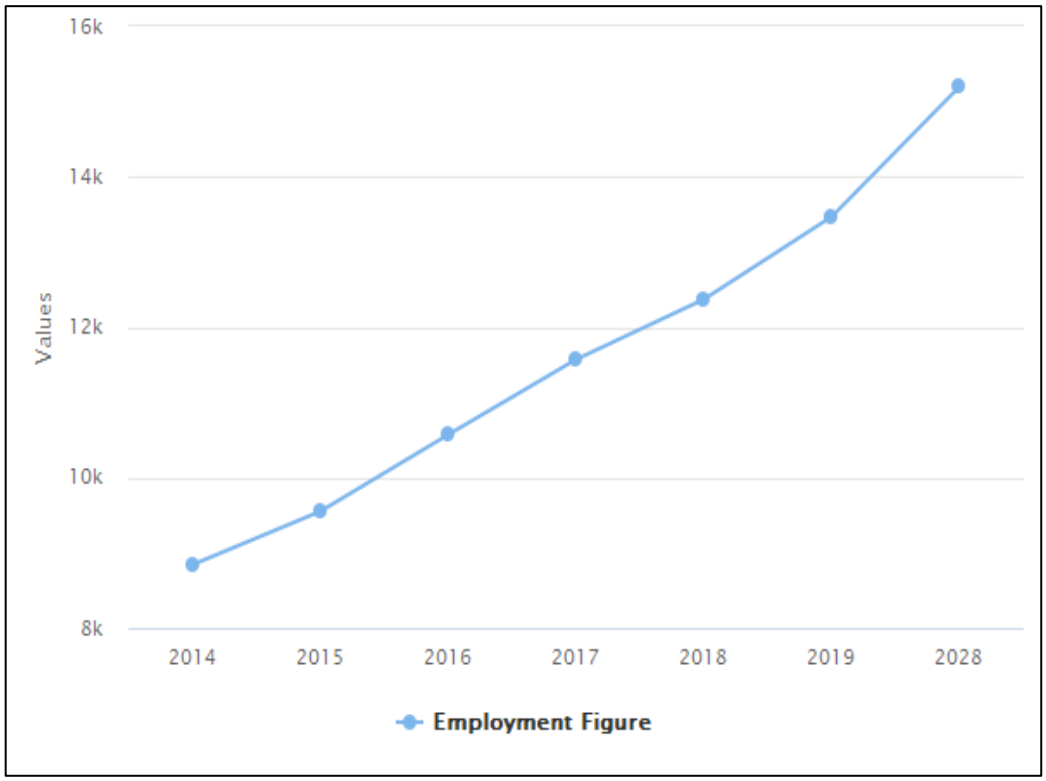
cybersecurity skills; cybersecurity education; cybersecurity curriculum; KSA; non-technical skills; cybersecurity training; cybersecurity roles; cybersecurity workforce, cybersecurity professional development, remote internship; educational innovation

INTRODUCTION

Long before the COVID-19 pandemic, cybersecurity workers felt the pressure of being understaffed despite aggressive actions to hire people with the right expertise (Crumpler & Lewis, 2019). The COVID-19 pandemic exacerbated the need for workers as people went online to work, play, and learn remotely. From March of 2019 and for years afterward, reports of cyberattacks, social engineering scams, identify theft, and cyber-based financial fraud skyrocketed and frequently made news headlines (FBI, 2020, June 9; USSS, 2020, March 9). This perfect storm of an almost ubiquitous online presence globally for workers, learners, and everyday users exacerbated the shortage of required cybersecurity professionals (BLS, 2020, July 2) (Figure 1).

Figure 1

Burning Glass Demand for Cybersecurity Workers Growth Data



Note: Burning glass Information Security Analyst Expected Job Growth over next 10 Years

With the increased home, learning, and business activity online came a corresponding surge in cybercrime (USSS, 2020, March 9). The Federal Bureau of Investigation (FBI) COVID-19 Working Group, in conjunction with the Secret Service's Global Investigative Operations Center (GIOC), reported that COVID-19 related cybercrime accounted for a 300 percent jump in complaints in the first four months of the COVID-19 pandemic (FBI, 2020, June 9). The pandemic heightened the need for corporate, academic, and government institutions to work together to figure out better ways to attract and retain cybersecurity professionals despite being forced to keep socially distant. Students were aware of the tremendous opportunities in cybersecurity and looked for enhanced entry skills.

The University of Southern Maine (USM) Department of Technology developed the Cybersecurity Ambassador Program (CAP) with the workforce and students' demands in mind. The graduate and undergraduate cybersecurity programs were growing because students saw the opportunity. Then, and now, there were thousands of unfilled jobs throughout New England, where the median salary was $101K (BLS, n.d.). However, this need for workers did not translate into more cybersecurity internship jobs for students. Observational data suggested that there were fewer jobs at the beginning of the COVID-19 pandemic as companies struggled to manage workers in virtual teams. It was not until a year later that more virtual internship jobs appeared, signaling that companies now had the tools, training, and time to pivot from teaching their workers to including interns.

During the intern job dry spell, the students expressed concerns that they would not get the requisite internship needed for graduation requirements. In addition, the faculty observational data noted that students from underrepresented populations, including women, people of color, and international students, were particularly disadvantaged in seeking internship roles. For this reason, researchers secured grant funding to pursue a reinvention of cybersecurity internships that benefitted the students and community.

The work done by the National Initiative for Cybersecurity Education (NICE) provided the framework for the program. The published knowledge, skills, and abilities (KSAs) from NICE and the National Security Agency (NSA) guidelines for Centers for Cybersecurity Academic Excellence – Cyber Defense (CAE-CD) provided the curriculum foundation. The purpose of the inquiry was to explore how to create an enrichment program that was not duplicative of classroom instruction. Instead, the intention was to increase the participants' workforce readiness and increase community cyberinfrastructure (CI) literacy, particularly for vulnerable populations.

The faculty vision for CAP was to immerse students in scholarly cybersecurity research. This immersion established baseline knowledge and served as a principal means to assure quality for these workshop presentations to the community. The workshop preparation curriculum involved NICE delineated soft, hard, and mixed non-technical skills deemed most important by cybersecurity hiring managers (Sussman, 2020) (Table 1).

Table 1

Prioritized List of Non-technical Skills Based on Cybersecurity Hiring Manager Data

Nodes	Skills
Soft competencies	Presentation skills
Soft competencies	Developing positive customer relations
Mixed competencies	Critically using information for decision making
Soft competencies	Customer Service Problem Resolution
Soft competencies	Written communications skills
Soft competencies	Working effectively with peers
Hard competencies	Knowledge of core business processes
Soft competencies	Facilitating teams and teamwork
Soft competencies	Intellectual curiosity
Hard competencies	Using computers effectively
Hard competencies	Knowledge of and compliance with legal and regulatory requirements
Soft competencies	Adaptability
Soft competencies	Professional demeanor
Soft competencies	Negotiating techniques
Hard competencies	Managing crisis situations
Mixed competencies	Training
Soft competencies	Ethics in decision making
Soft competencies	Managing personal stress
Soft competencies	Leadership abilities

Note: These Knowledge, Skills, and Abilities (KSAs) are based on data from NICE and CAE-CD

The program leaders asked the students to create writing, presentation, and multimedia artifacts based on researcher data. Finally, the faculty mapped the CAP curriculum to the NICE competencies in a sequential and progress framework (Table 2).

Table 2

NICE Non-technical Skills KSAs Mapped to the Cybersecurity Ambassador Curriculum

Curriculum Level	Nodes	Skills
Bronze	Soft competencies	Presentation skills
Bronze	Soft competencies	Developing positive customer relations
Bronze	Soft competencies	Written communications skills
Bronze	Soft competencies	Working effectively with peers
Bronze	Soft competencies	Intellectual curiosity
Bronze	Hard competencies	Using computers effectively
Bronze	Soft competencies	Adaptability
Bronze	Soft competencies	Professional demeanor
Bronze	Mixed competencies	Training
Bronze	Soft competencies	Ethics in decision making
Bronze	Soft competencies	Managing personal stress
Silver	Soft competencies	Customer Service Problem Resolution
Silver	Hard competencies	Knowledge of core business processes
Silver	Hard competencies	Knowledge of legal and regulatory requirements
Silver	Hard competencies	Managing crisis situations
Gold	Mixed competencies	Critically using information for decision making
Gold	Soft competencies	Facilitating teams and teamwork
Gold	Hard competencies	Compliance with legal and regulatory requirements
Gold	Soft competencies	Negotiating techniques
Gold	Soft competencies	Leadership abilities

The CAP students used these deliverables directly and in supplemental fashion in their workshops to organizations that fit the vulnerable population parameters established at the program's start.

CAP started the undergraduate student training focused on their ability to master and present four introductory seminars. These fifteen-minute workshops include phishing, identity protection, social media safety, and everyday home cyber safety. Every student learns the base information and expectations. They then learn to tune information and handouts based on the demographics of the organization receiving the training. As they progress through the curriculum, they earn micro-credentials indicating they are either a bronze, silver, or gold level Cybersecurity Ambassador. The Faculty Advisor, Graduate Assistants (GAs), and senior Cybersecurity Ambassadors (CAs) mentor and coach the incoming cohort to ground them in the basics of these critical areas of cybersecurity awareness training.

Cybersecurity Ambassador Program (Cap) Evolution

There was not a great deal of budget to launch the CAP program. The faculty started with student volunteers. Unfortunately, that number dwindled due to competing work and study requirements. The faculty realized that CAP needed to provide students with work income to grow. The USM faculty advisor solicited public and private partners to fund internships. This funding methodology continues today. CAP advertises through the student employment center. An approved job description detailed the position and encouraged students from outside the cybersecurity undergraduate program to increase prospects from underrepresented populations. The faulty hired CAP's first Cybersecurity Ambassadors (CAs) funded by the Federal Work-Study (FWS) Program, University of Southern Maine (USM) grants, and using an allocated partial graduate assistantship.

The faculty then solicited organizations with common objectives concerning community awareness and training to avoid cyber-crime. The Maine Office of Securities provided a generous grant to jumpstart the program. Their only request was for USM to discuss financial risks as part of the outreach workshops. These initial funds allowed the faculty to create a marketing brand, use that branding for student incentives such as caps and shirts, purchase presentation equipment, and fund four one-semester internships.

The faculty advisor, supported by a part-time graduate assistant, hired CAs using the federal work-study program and grant-funded internships. They hired students interested or showed an aptitude for cybersecurity technology and wanted to work twenty hours each week during the semester. The faculty advisor created a three-tier program to allow those students who participated for more than one term to have scaffolded goals and objectives (Figure 2).

Figure 2

Cybersecurity Ambassador Program (CAP) Tiered Approach for Student Development

Cohorts of CAs achieved the first or bronze tier through oral and written assessments based on technical training and career planning modules developed and taught by working Cybersecurity researchers and Cybersecurity professionals. Students complete a self-assessment form and have an out-brief with the faculty advisor. They must also successfully present at least two of the four workshops. The second (silver) phase emphasized leadership and mentorship and required students to deliver on the four core areas. The advisor and graduate assistant assessed CA's presentation skills, leadership, collaboration, and research efforts based on their workshop work, handouts, and other artifacts. Finally, CAs achieved the top (gold) level when they could help coordinate outreach and certify other students.

It cannot be overstated that the vision was to promote sought-after cybersecurity workplace skills for students while simultaneously giving back to the community. At the same time, this program provided access and support to students from historically underrepresented populations in the Information Security and Cybersecurity disciplines. For example, we found that international and minority cybersecurity students applied for the CAP internship citing difficulty getting hired by outside entities. One area for future study is determining if bias forms barriers for students from underrepresented populations

in cybersecurity to get outside internship opportunities. Regardless, CAP provided a means for these minority students to earn internships needed to graduate from the USM cybersecurity undergraduate program.

The first CA cohorts spent most of their time understanding the current cybersecurity-related trends and how to promote awareness of those trends to at-risk communities in Maine. We fostered an open work environment where asking questions became core to helping the overall team understand what they could do to help each other. The students quickly created a social platform on Discord to facilitate chats between members. We used a shared Google drive to create, collaborate, and archive scholarly and presentation artifacts.

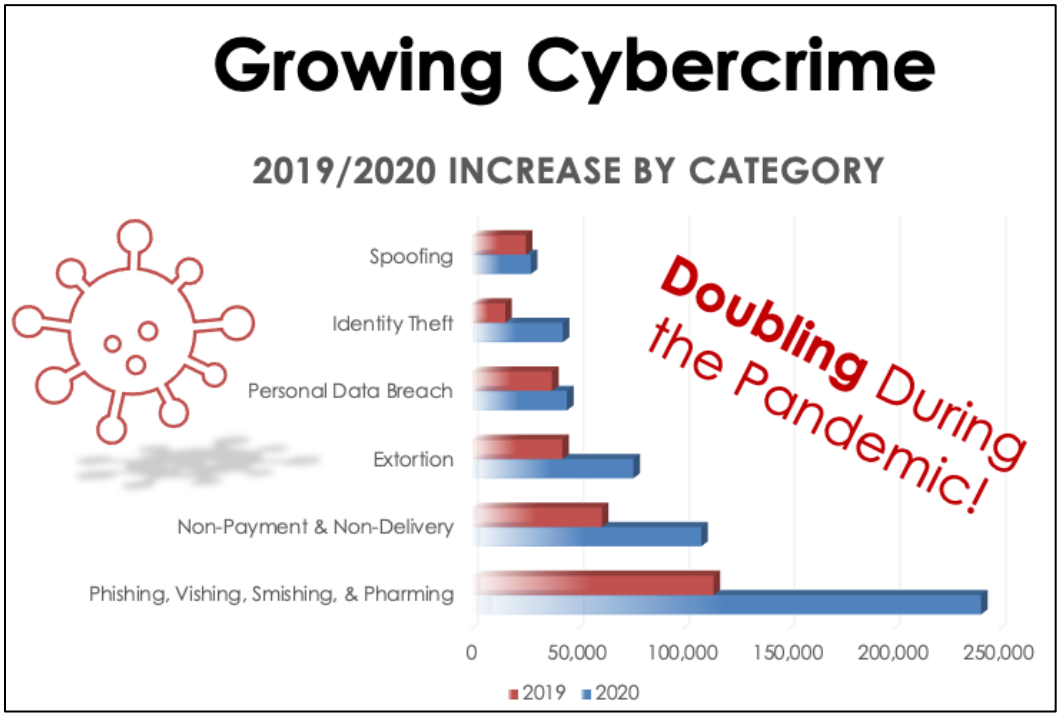
CAP initially intended to employ students with a keen technical understanding of cybersecurity and build upon their knowledge. The faculty did not envision a program beyond hiring STEM students who entered with foundational cyber knowledge, skills, and abilities (KSAs). However, the COVID-19 pandemic made the leaders broaden their focus. The introduction of students from complementary fields helped develop the sought-after non-technical skills. Conversely, the cybersecurity students broadened the other students' outlooks regarding cybersecurity. In this way, the expansion of the program improved outcome attainment.

The Cybersecurity Ambassador Program's objective was, and remains, to provide students with immersive experiences and exposures to cybersecurity awareness and to train research that complimented their cybersecurity KSAs as they produced community awareness training for vulnerable populations. However, by expanding opportunities for students outside the cybersecurity program, we have enhanced the overall productivity and expanded the possible workforce talent pool. Also, this enrichment accelerates students' transition to practice regardless of field. Finally, the program’s applied projects assist with accreditation attainment as the NICE outcomes dovetail with CAE-CD sanctioned objectives. As such, employers, accreditors, and clients see the program's value as students apply what they know about social engineering, privacy, and interventions to thwart cybercrime.

The CAP team looked at the FBI (2020, 2019) Internet Crime Reports and continued using such government data to keep the four key cybersecurity workshop areas up to date. As the data revealed, these topics creating awareness about phishing, identity/privacy, cyber safety, social media safety, and cyber home safety were and remain relevant (Figure 3).

Figure 3

Top Cybercrime Reported to the FBI in 2019 and 2020



Note: Figure derived from the FBI 2019 and 2020 Internet Crime Reports.

We realized that we could not wait for the pandemic to recede when we first started. In addition, cybercrime incidents doubled in 2019, and this data increased the faculty's urgency to get a remote model operational.

Maine is a very rural state but still experienced a significant rise in cybercrime (Figure 4).

Figure 4

Maine Cybercrime Reported to the FBI in 2019 and 2020

Maine vs. National Losses

	MAINE		NATIONAL	
Age Range	Count	Losses	Count	Losses
Under 20	47	$298,227	23,186	$70,980,763
20 - 29	163	$78,519	70,791	$197,402,240
30 - 39	248	$694,123	88,364	$492,176,845
40 - 49	211	$706,649	91,568	$717,161,726
50 - 59	263	$1,792,048	85,967	$847,948,101
Over 60	368	$2,471,681	105,301	$966,062,236

Note: Figure derived from the FBI 2019 and 2020 Internet Crime Reports.

The CAP CAs mined Maine crime data to provide facts and data in their presentations. The intention was to get students to tailor general workshops to increase significance to the organization receiving the training event.

CAP also provided opportunities for students to apply their knowledge as leaders. Although CAP is faculty-led, it is a student-driven organization dedicated to raising cybersecurity awareness in high-risk groups throughout Maine. It provides interested students opportunities to participate in cybersecurity awareness and education research, organize that research into presentations, and deliver this content to those at-risk individuals and organizations who request support. Students who participated in the program got a unique opportunity to give back to their communities, develop highly sought-after workplace skills in the field of cybersecurity, and build their confidence in conveying complex concepts to non-technical participants.

Students continue to run CAP workshops that focus on phishing, social media safety, online identity protection, and cyber home safety. The students share tips, tricks, and information to help participants evade disruptions due to cybercriminal activity. In addition, the CAP students help Maine residents with practical advice on protecting their privacy, identity, and financial information. Many Maine

residents face the challenges of not knowing what steps they can take to avoid cyberattacks, and CAP students help them feel more empowered based on shared information. The feedback is that the student workshops are highly effective in helping these vulnerable groups avoid being victimized.

Continuing Cap in The New Normal

This year Governor Janet Mills signed an executive order establishing a cybersecurity advisory panel "to strengthen the security and resiliency of the State's information technology infrastructure to protect against cyber risks and ensure effective cybersecurity communications" (Maine Exec. Order No. 2021-25, 2021, January 13, p. 1). This executive order codifies the urgency surrounding synchronizing cybersecurity efforts to identify, mitigate, and detect Maine citizens' cybersecurity risks. However, many Mainers do not know where to start to identify, mitigate, and report cybercrime. CAP provides education and information to protect Maine's vulnerable populations. We intend to keep the virtual team format going forward but include more in-person opportunities as the pandemic subsides. Thus, eventually, CAP will have a blended versus entirely virtual modality.

CAP is also a relationship-based program despite the remote modality. The CAP team meets weekly at the beginning of the week to gauge progress, discuss tasks, and prepare for upcoming workshops. In addition, the GA charged with student coordination meets with each participant one-on-one weekly to provide encouragement and review deliverables. The Dean awarded CAP with a second part-time GA position in AY2021-2022. The new GA was charged with content coordination and oversight for more complex collaboration, ensuring product outcome quality. The program continues to have students collaborate using online conferencing and collaboration tools such as Zoom, Trello, CANVA, Zotero, Discord, and shared drives. Their experience as remote workers using various tools strengthens independence and interdependence.

Students are central to this program and work with cybersecurity experts as coaches and advisors. This cybersecurity education, training, and awareness research enhance the students' technical and non-technical education through career mentoring. USM CAP provides direct mentoring of undergraduate and graduate students with active Cybersecurity researchers and professionals. A diverse group of researchers/community professionals provides training in Cybersecurity domains that include:

1) Securing personally identifiable information,
2) Securing the internet of things,
3) Social media safety,

4) Internet risks,
5) Cybersecurity incident response,
6) Cybersecurity governance, policy, and legislation.
7) Cybersecurity ethical considerations.

Students perform research and produce artifacts used and shared throughout various communities in Maine that include organizations for older adults, K-12 and higher education students, and veterans, as just a few examples.

Said another way, the pandemic forced a virtual team model. However, this is a model readily used in the technology field. As such, CAP supports the integration of virtual learning and work.

This Cybersecurity Ambassador Program addressed the challenge of creating a trained and ready future cybersecurity workforce in general and in Maine in particular. This program promotes students' technical and professional skills to progress in the growing science, technology, engineering, and math (STEM) field while helping the community. Students learn that knowledge of cybersecurity issues alone is not enough to be work-ready. Effective communication is essential for dealing with non-technical clients. Our next steps will be to work with interdisciplinary faculty for increased student proficiencies skills that build interpersonal connections and productive relationships. At the same time, we have added the production of short videos and podcasts to expand CAPs outreach using new modalities. Finally, we continue to scout technology to enhance presentational speaking and communication facilitation skills for small groups and workshops. The research on the program's efficacy will continue to collect data to ensure the program’s effectiveness. However, at this time, the data shows that this pedagogical approach to curriculum development, grounded in the Ground Truth Expertise Development Model (GTEDM), is a unique methodology. This curriculum teaches cybersecurity interns with key non-technical but critical KSAs for cybersecurity professional development has proved to be a factor in accelerated hiring for program participants.

REFERENCES

Assante, M. J., and Tobey, D. (2011). Enhancing the cybersecurity workforce. IT Professional 13(1), 12-15, doi 10.1109/MITP.2011.6

Association of American Colleges and Universities (AACU). (n.d.). VALUE Rubrics. https://www.aacu.org/value-rubrics

Blair, J. R. S., Hall, A. O., and Sobiesk, E. (2019, March). Educating future multidisciplinary cybersecurity teams. Computer 52(3), 58-66, doi: 10.1109/MC.2018.2884190.

Bloomberg, L. & Volpe, M. (2016). Completing your qualitative dissertation: A road map from beginning to end. 3rd Edition. Thousand Oaks, CA: Sage Publications.

Buchanan, B. G., Davis, R., Smith, R. G., & Feigenbaum, E. A. (2018). Expert Systems: A perspective from Computer Science. In K. A. Ericsson, R.R. Hoffman, A. Kozbelt, and A.M. Williams (Eds.) The Cambridge Handbook of Expertise and Expert Performance (2nd ed., pp. 84-104). Cambridge University Press.

Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry & research design: Choosing among five approaches.

Crumpler, W., and Lewis, J. A. (2019) The cybersecurity workforce gap. Center for Strategic & International Studies (CSIS). https://www.csis.org/analysis/cybersecurity-workforce-gap

Cybersecurity and Infrastructure Security Agency Act of 2018. 115 PL 278 132 Stat. 4168, 2018 Enacted H. R. 11-454 (2018). https://www.congress.gov/bill/115th-congress/house- bill/3359

Cybersecurity and Infrastructure Security Agency (CISA). (2020, April 27). Cybersecurity training and exercises. National Initiative for Cybersecurity Careers and Studies (NICCS). https://www.cisa.gov/cybersecurity-training-exercises

Cyberseek. (2020). Cybersecurity career pathway [Interactive data set on July 7, 2020]. https://www.cyberseek.org/pathway.html

Cyberseek. (2020). Cybersecurity Supply/demand heat map [Interactive data set on July 7, 2020]. https://www.cyberseek.org/heatmap.html

Dali'Alba, G. (2018). Reframing expertise and its development: A lifeworld perspective. In K. A. Ericsson, R.R. Hoffman, A. Kozbelt, and A.M. Williams (Eds.) The Cambridge Handbook of Expertise and Expert Performance (2nd ed., pp. 33-39). Cambridge University Press.

Deming, D. J. (2017). The Growing Importance of Social Skills in the Labor Market. The Quarterly Journal of Economics. 132 (4): 1593-1640.

Federal Bureau of Investigation (FBI). (2019). Internet Crime Report 2020. United States Department of Justice. https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf

Federal Bureau of Investigation (FBI). (2020). Internet Crime Report 2020. United States Department of Justice. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Federal Bureau of Investigation (FBI). (2020, June 9). News. COVID-19 fraud: Law enforcement's response to those exploiting the pandemic. United States Department of Justice. https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to- those-exploiting-the-pandemic

Giuseppe Croce & Emanuela Ghignoni (2020) The evolution of wage gaps between STEM and non-STEM graduates in a following technological economy, Applied Economics, 52:23, 2427-2442, DOI: 10.1080/00036846.2019.1691142

Haney, J. M., & Lutters, W. G. (2018). It's scary. it's confusing . it's dull": How cybersecurity advocates overcome negative perceptions of security. Proceedings of the Fourteenth Symposium on Usable Privacy and Security, Baltimore: MD, August 12-14, 2018. USENIX Association. https://www.usenix.org/conference/soups2018/presentation/haney- perceptions

ISC(2) (2019) Cybersecurity workforce study: Strategies for building and growing strong cybersecurity teams https://www.isc2.org/Research/2019-Cybersecurity-Workforce- Study#

Jang, H. (2016). Identifying 21st Century STEM Competencies Using Workplace Data. Journal of Science Education and Technology, 25(2), 284-301. Retrieved June 29, 2020, from www.jstor.org/stable/43867797

Lapena, R. (2017, October 17). Survey says: Soft skills highly valued by security team. Tripwire, https://www.tripwire.com/state-of-security/featured/survey-says-soft-skills-highly- valued-security-team/

Lapena, R. (2020, February 10). No relief for cybersecurity teams in sight, reveals Tripwire's latest skills gap report. Tripwire, https://www.tripwire.com/state-of-security/featured/tripwires-skills-gap-report/

Lee, L. (2019). Cybercrime has evolved: It's time cyber security did too. Computer Fraud and Security 2019(6), 8-11. https://www.sciencedirect.com/science/article/pii/S1361372319300636

Litecky, C. R., Arnett, K. P., & Prabhakar, B. (2004). The paradox of soft skills versus technical skills in is hiring. Journal of Computer Information Systems, 45(1), 69-76. doi:10.1080/08874417.2004.11645818

Maine Exec. Order No. 2021-25, Office of the Governor (January 13, 2021). Retrieved from https://www.maine.gov/governor/mills/sites/maine.gov.governor.mills/files/inline-files/EO%2082%2025.pdfMerriam, S. B., & Tisdell, E. J. (2016). Qualitative research: A guide to design and implementation (4th Ed.). San Francisco, CA: Jossey-Bass.

Mitchell, G. W., Skinner, L. B., & White, B. J. (2010). Essential soft skills for success in the twenty-first century workforce as perceived by business educators. Delta Pi Epsilon Journal, 52(1), 43-53.

Moustakas, C. (1994) Phenomenological research methods. Thousand Oaks, CA: SAGE. 800-181. US Department of Commerce. https://doi.org/10.6028/NIST.SP.800-181 National Institute of Standards and Technology. (n.d.). National Initiative for Cybersecurity Education {NICE} Cybersecurity Workforce Framework, Oversee and Govern. US Department of Commerce. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework?category=Oversee-and-Govern

National Institute of Standards and Technology. (n.d.). National Initiative for Cybersecurity Education {NICE}, National Initiative for Cybersecurity Education (NICE) Working Group (NICEWG). US Department of Commerce. https://www.nist.gov/itl/applied- cybersecurity/nice/about/working-group

National Research Council 2013. Professionalizing the nation's cybersecurity workforce?: Criteria for decision-making. Washington, DC: The National Academies Press.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST Special Publication (SP) https://doi.org/10.17226/18446.

Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (2018). Reassessment of expectations as a comparison standard in measuring service quality: Implications for further research. Journal of Marketing, 58(1), 111-124. doi:10.1177/002224299405800109

Petersen, R. (2019, November 12). NICE! 10 years in the Making. National Institute for Standards and Technology (NIST) [Blog]. https://www.nist.gov/blogs/cybersecurity- insights/nice-10-years-making#:~:text=While%20the%20inception%20of%20NICE,held%20until%20two%20yea rs%20later.

Ravitch, S. M., & Riggan, M. (2017). Reason & rigor: How conceptual frameworks guide research. (2nd ed.). Thousand Oaks, CA: SAGE Publications.

Roberts, C. M. (2010). The dissertation journey. A practical and comprehensive guide to planning, writing, and defending your dissertation (2nd ed.). Thousand Oaks, CA: Corwin, A SAGE Publication.

Saldana, J. (2016). The coding manual for qualitative researchers (3rd ed.). Thousand Oaks, CA: SAGE.

Sandwith, P. (1993). A hierarchy of management training requirements: The competency domain model. Public Personnel Management, 22(1), 43-62. https://doi.org/10.1177%2F009102609302200104

Sisson, L. G. & Adam, A. R. (2013). Essential hospitality management competencies: The importance of soft skills, journal of hospitality & tourism education, 25(3), 131- 145, DOI: 10.1080/10963758.2013.826975

Sussman, L. L. (2020). Exploring Non-Technical Knowledge, Skills, and Abilities (KSA) that May Expand the Expectations of the Cyber Workforce. National CyberWatch Center Digital Press ID NCC-2020-CSJ-02 Cybersecurity Skills Journal. National Cyberwatch Org, 19.

Tobey, D. (2012). Smart grid cybersecurity: Job performance model report, NBISE technical report, SGC working group 12-01 Draft. National Board of Information Security Examiners.

US Bureau of Labor Statistics (BLS). (n.d.). Occupational Outlook Handbook. US Department of Commerce. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

US Bureau of Labor Statistics (BLS). (2020, July 2). News Release, The employment situation - June 2020. US Department of Commerce. https://www.bls.gov/news.release/pdf/empsit.pdf

US Bureau of Labor Statistics (BLS). (2020, April 10). Occupational Outlook Handbook, Computer Support Specialists. United States Department of Labor. https://www.bls.gov/ooh/computer-and-information-technology/computer-support- specialists.htm

US Bureau of Labor Statistics (BLS). (2020, April 10). Occupational Outlook Handbook, Customer Service Representative. United States Department of Labor. https://www.bls.gov/ooh/office-and-administrative-support/customer-service-representatives.htm#tab-2

US Bureau of Labor Statistics (BLS). (2020, April 10). Occupational Outlook Handbook, Information security analysts. United States Department of Labor. https://www.bls.gov/ooh/computer-and-information-technology/information-security- analysts.htm

U.S. Bureau of Labor Statistics (BLS). (2020, April 23, 2020). TED: The Economics Daily, Unemployment rates rose in 29 states and the District of Columbia in March 2020. U.S. Department of Labor. https://www.bls.gov/opub/ted/2020/unemployment-rates-rose- in-29-states-and-the-district-of-columbia-in-march-2020.htm#:~:text=Bureau%20of%20Labor%20Statistics,-The%20Economics%20Daily&text=Twenty%2Dnine%20states%20and%20the,to%204.4%20percent%20in%20March.

United States Continental Army Command (USCAC). (1968). Regulation 350-100-1, Training. Fort Monroe, VA. https://stacks.stanford.edu/file/druid:tv440px2527/tv440px2527.pdf

U.S. Secret Service (USSS). (2020, March 9). Secret Service issues COVID-19 {COVID-19} phishing alert, [Press Release]. U.S. Department of Treasury. https://www.secretservice.gov/data/press/releases/2020/20-MAR/Secret_Service_COVID-19_Phishing_Alert.pdf

Winegard, B., Winegard, B., and Geary, D. C. (2018). The evolution of expertise. In K. A. Ericsson, R.R. Hoffman, A. Kozbelt, and A.M. Williams (Eds.) The Cambridge Handbook of Expertise and Expert Performance (2nd ed., pp. 40-48). Cambridge University Press.

World Economic Forum. 2016. The future of jobs, employment, skills, and workforce strategy for the fourth industrial revolution. Geneva. http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf

Yin, R. K. (2018). Case study research and applications: Design and methods. (6th ed.). Thousand Oaks, CA: SAGE Publications.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F. & Basim, H. M. (2020): Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, Journal of Computer Information Systems, DOI:10.1080/08874417.2020.1712269