IMPLEMENTING COLLEGE TO WORK PIPELINE IN CYBERSECURITY: A COMMUNITY COLLEGE PERSPECTIVE

Rosalyn Warren

INTRODUCTION

There is a national shortage of IT talent. As a result, some employers have modified their recruitment requirements to attract skilled IT professional such as lessening degree requirements in favor of industry-specific certifications to appeal to a larger demographic (Fuller, et al., 2022; Wilkinson, 2022). The Office of Federal Procurement Policy encourages federal offices "to limit the use of educational requirements in favor of stated skills when acquiring information technology (IT) services" (Wooten, 2021). As more employers are relying on IT certifications to validate technical skills, community colleges must be prepared to provide a quick solution.

Currently, there are three options for achieving an entry-level IT job: learning in-demand skills, earning industry certifications, and graduating with a college degree. Although approximately 60% of entry-level cybersecurity jobs require a college degree in a related field (Marquardson & Elnoshokaty, 2020), financial and time constraints often make IT certifications and boot camps more favorable than earning a degree (Amsier, 2021; Marquardson & Elnoshokaty, 2020; Perry, 2023). Also, 63% of US companies stated *industry-recognized IT certifications* are valuable in the hiring process (Sava J. A., 2022b). Nevertheless, a student with IT certifications and a degree has a better chance for long-term career success (Randall & Zirkle, 2023).

The computer information science (CIS) department at Enterprise State Community College (ESCC), a 2-year college located in southeast Alabama, is charged with preparing the next generation of IT professionals for entry-level positions. ESCC has partnered with local organizations and has joined IT academies to improve available resources to students.

OBJECTIVES

Recognizing the value of a degree and industry certification, ESCC has revamped its curriculum to combat the IT shortage (Statista Research Department, 2023), the CIS curriculum at ESCC will include the following:

- Embed DoD Approved 8570 Baseline Certifications within the CIS degree options.
- Become designated by the National Security Agency as a National Center of Academic Excellence in Cyber Defense (NCAE-CD).
- Earn Computing Accreditation Commission (CAC) accreditation by the Accreditation Board for Engineering and Technology (ABET) for ESCC's Information Security and Assurance program.
- Gain Accreditation Council for Business Schools and Programs (ACBSP) accreditation for the CIS program
- Strengthen collaborative efforts with local schools
- Include NIST Special Publication 800-53 in the CIS curriculum

1. Cybersecurity and Infrastructure Security Agency's (CISA) National Initiative for Cybersecurity Careers and Studies (NICCS) Training Provider
2. IBM
3. RedHat Academy
4. AWS Partner Network
5. CYBER.ORG (K-12 only)
6. Ncyte Educational Member
7. Oracle Academic Partner
8. CompTIA Academic Partner
9. Cisco Networking Academy
10. EC-Council Academia Partner
11. Microsoft Learn for Educators
12. Palo Alto Cybersecurity Academy
13. VMWare IT Academy
14. National Cyberwatch Center Member
15. US Cybercom's Academic Engagement Network
16. Fortinet Academic Partner
17. GitHub Education
18. Skillstorm
19. Advantage Consulting and Solutions LLC

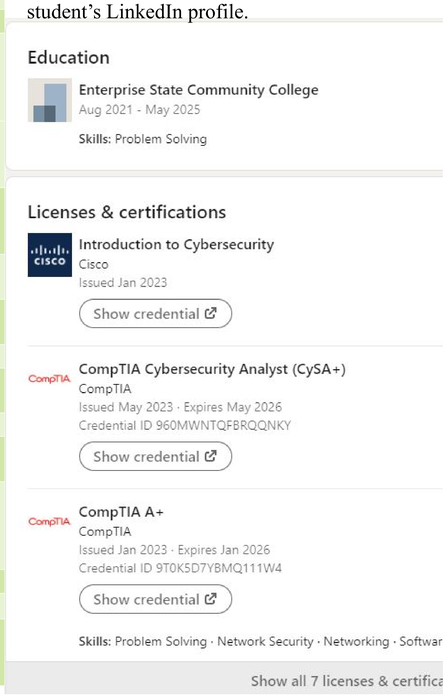
ESCC is working with 19 organizations with the goal of including vendor-specific and vendor neutral content into the CIS courses. The alliances provide free and academic discounts on the IT certification vouchers. In addition, the organizations provide free resources such as software, virtual machines, and instructor guides. Local organizations provide experiential learning opportunities. Content from multiple sources and combined in a course; therefore, students frequently earn several badges and certifications in a single course. Micro-credentials are used for exams and a certification exam is the final exam. CIS courses use NIST 800-53 as a reference. Below is a list of CIS courses and the certifications and badges for the course:

Course	IT Certifications	IT Badges
CIS 134	1. CompTIA IT Fundamentals+ 2. NSE1 3. NSE2	
CIS 150	Python Institute Certified Entry-Level Python Programmer (Exam PCEP-30-0x)	
CIS 161	1.EC-Council E|HE Ethical Hacking 2.N|DE Network Defense Essentials 3.NSE3	1.Cisco Networking Badge 2.Cisco Packet Tracer
CIS 162	1.CompTIA Network+ 2. NSE4 3.NSE5	1.Cisco Networking Devices & Initial Configuration 2.Cisco Network Addressing & Basic Troubleshooting
CIS 17I	Red Hat Certified System Administrator (RHCSA)	
CIS 196	Microsoft Azure Data Fundamentals (DP-900)	
CIS 211	CompTIA CySA+ •SASE Expert Certification - Level 1 •SASE Expert Certification - Level 2 •SASE Advanced Security Cert	Palo Alto Networks Micro-Credential for Virtual Network Security Administrator
CIS 230	1.EC-Council D|FE Digital Forensics Essentials 2.SASE Business Impact & Strategy 3.NSE6	Cisco Cyber Threat Management
CIS 231	1.EC-Council E|CIH Certified Incident Handler 2.SASE Deployment & Management 3.NSE7	
CIS 246	EC-Council Certified Ethical Hacker	
CIS 255	Oracle Java Foundations Certified Junior Associate (1Z0-811)	
CIS 256	Oracle Java EE 7 Application Developer 1Z0-900	
CIS 260	CompTIA Security+	
CIS 268	CompTIA A+	
CIS 269	CompTIA A+	
CIS 275	Azure Administrator Associate (AZ-104)	1.Cisco OS Basics 2.Palo Alto Networks Micro-Credential Remote User Administrator (PMRuA)
CIS 276	MS-900	
CIS 277	MS-500	
CIS 292	Microsoft Azure Security Technologies (AZ-500)	Palo Alto Networks Micro-Credential Remote User Administrator (PMRuA)

The academic discounts and free learning resources makes earning IT certifications affordable for our students. ESCC is able to sell the IT vouchers in the campus bookstore.

ESCC implemented Google Professional Certifications via Coursera.

CIS students are required to create a LinkedIn account and list their certifications and badges as they progress through the program. Below is a section of an ESCC student's LinkedIn profile.



METHODS

The implementation of certifications and partner resources were implemented in the Spring semester of 2023. CIS courses at ESCC used the NIST 800-53 as a reference. In addition, courses also included a combination of resources from Coursera, Cengage, and IT academic academy (academies varied by course). Throughout the course, students were required to complete a micro-credential such as a Cisco Cyber Threat Management in CIS 211. Instead of traditional exams, students were to earn a vendor specific certification such as SASE Expert Certification for CIS 211. The learning resources consisted of CompTIA CySA+ Student Guide, CertMaster Labs, onlinevideos and other resources. In CIS 211, students who had an average of 80% or above, received a free voucher to take the CompTIA CySA+ exam as their final exam. Students who did not meet the requirements, took a comprehensive final exam.

RESULTS

Of the 10 students in CIS 211 who took the CySA+ exam, 3 students passed the exam. The students who did not pass the exam earned an average score of 637 (on a scale of 100 to 900). The lowest score on the exam was 604. Because Spring 2023 was the first semester the resources were implemented, many of the students did not have ample courses to build a solid foundation.

CONCLUSION

The results indicated that the CIS department needs to do more to prepare students for earning industry certifications in IT. The following measures were implemented based on the results:

- Internal and external student-centered study groups were formed
- Prerequisites were enforced
- Improved collaboration between local high schools
- The development of an IT club

The implementation of the measures will improve student outcomes and poise the CIS program to earn accreditation from various bodies.

REFERENCES

To access the full list of references, use your smart device to scan the QR code.

ENTERPRISE STATE
COMMUNITY COLLEGE