Journal of Cybersecurity Education, Research and Practice

Volume 2023 | Number 2 Article 2

October 2023

Integrating certifications into the cybersecurity college curriculum: The efficacy of education with certifications to increase the cybersecurity workforce

Binh Tran
Georgia Gwinnett College, btran5@ggc.edu

Karen C. Benson
Georgia Gwinnett College, kbenson4@ggc.edu

Lorraine Jonassen
Georgia Gwinnett College, ljonassen@ggc.edu

Recommended Citation

Tran, Binh; Benson, Karen C.; and Jonassen, Lorraine (2023) "Integrating certifications into the cybersecurity college curriculum: The efficacy of education with certifications to increase the cybersecurity workforce," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2023: No. 2, Article 2.
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss2/2

Integrating certifications into the cybersecurity college curriculum: The efficacy of education with certifications to increase the cybersecurity workforce

Abstract

One only needs to listen to the news reports to recognize that the gap between securing the enterprise and cybersecurity threats, breaches, and vulnerabilities appears to be widening at an alarming rate. An untapped resource to combat these attacks lies in the students of the secondary educational system. Necessary in the cybersecurity education is a 3-tiered approach to quickly escalate the student into a workplace-ready graduate. The analogy used is a three-legged-stool, where curriculum content, hands-on skills, and certifications are equal instruments in the edification of the cybersecurity student. This paper endeavors to delve into the 3rd leg of the stool by developing the concept of vendor-specific and vendor-neutral certifications to educate the cybersecurity student and test their capability of protecting the workplace. The research data was drawn from companies in the Atlanta, Georgia area, who employ and hire cybersecurity recruits. The data from the research proves certifications are necessary as an addition to the cybersecurity curriculum in the secondary education arena. The paper reviews the need for cybersecurity graduates, the balance between cybersecurity theory and applied skillsets, the difference between a certificate and a certification, benefits to the community, classifications of certifications, relevancy of a college degree in today's workforce, and recommendations for further study.

Keywords

certifications, certificate, hands-on learning, cybersecurity, curriculum development in cybersecurity, college degree vs. certification

Integrating certifications into the cybersecurity college curriculum

Binh Tran
Georgia Gwinnett College
btran5@ggc.edu
0009-0005-4523-4040

Karen C. Benson
Georgia Gwinnett College
kbenson4@ggc.edu
0000-0002-3087-5495

Lorraine Jonassen
Georgia Gwinnett College
ljonassen@ggc.edu
0000-002-3928-9767

Abstract— One only needs to listen to the news reports to recognize that the gap between securing the enterprise and cybersecurity threats, breaches, and vulnerabilities appears to be widening at an alarming rate. An un-tapped resource to combat these attacks lies in the students of the secondary educational system. Necessary in the cybersecurity education is a 3-tiered approach to quickly escalate the student into a workplace-ready graduate. The analogy used is a three-legged- stool, where curriculum content, hands-on skills, and certifications are equal instruments in the edification of the cybersecurity student. This paper endeavors to delve into the 3rd leg of the stool by developing the concept of vendor-specific and vendor-neutral certifications to educate the cybersecurity student and test their capability of protecting the workplace. The research data was drawn from companies in the Atlanta, Georgia area, who employ and hire cybersecurity recruits. The data from the research proves certifications are necessary as an addition to the cybersecurity curriculum in the secondary education arena. The paper reviews the need for cybersecurity graduates, the balance between cybersecurity theory and applied skillsets, the difference between a certificate and a certification, benefits to the community, classifications of certifications, relevancy of a college degree in today's workforce, and recommendations for further study.

Keywords— certifications, certificate, hands-on learning, holistic education, cybersecurity, curriculum development in cybersecurity, college degree vs. certification

I. Introduction

Institutes of Higher Learning (IHLs) routinely use cybersecurity certifications in their curriculum; however, not much is mentioned about the verifiable results for greater opportunities with employment in the systems and cybersecurity fields. To make a case for increased usage of cybersecurity certifications in the curriculum, viable data must be gathered to ascertain the efficacy of certifications relevant to workplace opportunities in the cybersecurity arena. Inspection of the data will aid instructors and administrators in making calculated curriculum decisions based on statistical analysis instead of current marketing trends. Such data can be instrumental in weaving the theory of cybersecurity with practice exam questions to prepare the student for certifications. For example, combining the theory of the 7-domains of IT infrastructure with practical, relevant questions found in past certifications on the domains [24]. Currently, there exists a research gap between those students holding a cybersecurity certification and their hiring outcomes, as there are no prior studies in this area.

The volatility of the cybersecurity workforce is as changing as the insurmountable number and forms of security breaches that are reported each day. However, the constant in the equation is the need for qualified cybersecurity professionals who are trained by Subject Matter Experts (SMEs) and tested by certifications applicable to the student's degree. This paper will endeavor to show data from Atlanta Georgia businesses who hire cybersecurity recruits and interns. The research found that the businesses interviewed desired certifications, coupled with a 4-year degree, when looking for a potential employee for cybersecurity job placement. Moreover, the paper will analyze the topic through the multiple lenses of: 1) current peer-review studies on cybersecurity certifications, 2) types of cybersecurity certifications, 3) evaluation of the data obtained from the graduates and corporate affiliates, and 4) recommendations for future research on cybersecurity certifications in IHLs. The information from this paper can be used to formulate a more robust cybersecurity curriculum and be a catalyst for future, formulative research into certifications and secondary education.

II. Need for Cybersecurity Professionals

The demand for cybersecurity analysts has grown exponentially due to the increasing number and innovative attacks that occur on the U.S. infrastructure, businesses, and governmental agencies [29], [3]. The paradigm shift to remote work places, the advance of Internet of Things (IoT), and the growth of e-commerce has widened the gap between threat attacks and security professionals. As reported by [15], 464,000 workers were added to the cybersecurity workforce in 2022; however, the gap in cybersecurity professionals has grown twice as much. In 2022, approximately 22 billion personal records were exposed to hackers in the 4,100 publicly reported data breaches [23]. This figure is expected to grow by 5% in 2023. These include attacks on Uber, Twitter, student loan accounts, and credit card accounts. The [15] estimated global cybersecurity workforce at 4.7 million people; yet, to thwart the increasingly innovative and destructive threats, government and organizations must have 3.4 million more workers globally. More than 70% of organizations report the lack of proficient cybersecurity professionals, placing the organizations at extreme risk of cyber-attacks and shutdowns [5]. A recent poll of IT executives found 67% of companies require cybersecurity certifications as an entry requirement to hiring. In a separate survey, 80% of IT professionals stated cybersecurity certifications are useful in their on-going careers [9].

How can we as educators minimize this gap between need and availability in the cybersecurity arena with our college graduates in cybersecurity? What tools are needed to meet the challenge of the cybersecurity regulatory demands and combatting innovative threat activists? The future requires IT professionals to evolve with the volatility of the cybersecurity threat landscape. As educators, we must break free from our traditional teaching style of memorize-test-forget and be innovative in our instructional delivery with experiential learning and industry certifications. Furthermore, the educator must constantly stay abreast of the modern cyber-attacks and threats to parlay the knowledge to the student, and thereby, enhance cybersecurity in the workplace.

III. BALANCE BETWEEN CERTIFICATIONS AND APPLICABLE SKILLS

The importance of cybersecurity skills and theoretical knowledge in the IHL cybersecurity student cannot be understated. However, what skills are needed by the current workforce, how are these skills taught, and how is the degree of student comprehension measured? Currently, there are 3 million workers in the cybersecurity workforce [1], [4], [2]. Due to the ever-advancing strategy of cyber-attacks, security educators must adapt their curriculum and teaching methodology at an increasing pace to propel the student into a workplace-ready skillset for cybersecurity. To maintain relevance in the cybersecurity field, certain topics must be continually upgraded: 1) faculty cybersecurity knowledge on the latest threats, 2) student hands-on skills, and 3) reinforcing student outcomes with certifications [13]. The skills gap has doubled with a 3.5 million shortage of cybersecurity jobs in 2021 and even greater in 2022 [20]. Accordingly, the static nature of academic curriculum tends to enlarge the gap between needed skills in the cybersecurity industry and IHL student graduates. The current curriculum framework consists of a silo learning approach where students learn only generic skillsets on a single topic [12]. For example, in the silo approach, possible coursework may focus on software platform security but then ignore the human factor involved in protecting the organization's software and data. A more synergistic approach to teaching the IHL student is necessary to decrease the skills *vs*. workforce gap, as universities are under greater pressure to produce graduates with a deeper level cybersecurity knowledge. The synergy between textbook content taught in the classroom, problem solving skills, and critical thinking cannot be underestimated in the cybersecurity field [16].

A part of the approach to maintain the latest standard in cybersecurity curriculum and to move from the static/silo curriculum to the constantly shifting landscape of threats is the implementation of professional certifications into the IHL curriculum [13]. Governing bodies that create the certifications, for example, CompTIA, are motivated to derive questions for the certification that exemplify relevant threats and attacks in the current environment [16].

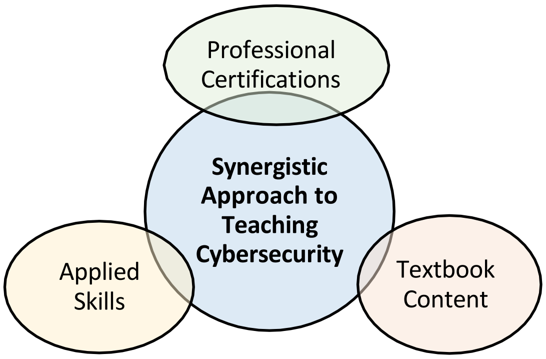
Professional Certifications
Synergistic Approach to Teaching Cybersecurity
Applied Skills
Textbook Content

Figure 1. Keys to a Synergistic Approach to Teaching Cybersecurity in an IHL

To maintain relevance in the competitive certification market, governing bodies must ensure their test questions and subject-matter content are pertinent to industry standards. Likewise, employers will search for candidates who have passed a certification in the employer's particular field of business. For instance, the applicant for the job may have passed CompTIA Security+, which demonstrates an entry level of security knowledge for the potential employer. According to [16], 35% of all cybersecurity positions will require applicants to pass certifications for employment. [15] found 58% of organizations are investing in certifications to prevent or mitigate cybersecurity staff shortages [15]. Effectively, more than half of organizations offer reimbursements for certifications in cybersecurity. The [11] research found that 94% of cybersecurity professionals believe their certifications helped them obtain employment and allowed them to protect their respective organizations more successfully. If passing a certification will gain an edge in the marketplace, why not integrate certifications in the current IHL curriculum?

Some academic viewpoints maintain that certifications, as a part of the curriculum, create an element of 'memorize and forget' when taking these exams, with the result of low-skilled job applicants in the workplace [16]. Admittedly, students may use the preparation of 'boot-camps' out of desperation to avail quick employment opportunities. To combat this occurrence, organizations routinely employ cybersecurity students based on these general assessment criteria: 1) academic degrees from an IHL, 2) professional/vendor specific certifications, 3) job or internship experience [14]. Instructors of cybersecurity in IHLs should balance in their curriculum the synergy between book knowledge, critical thinking skills, and pragmatic problem-solving skills. The complexity of securing the enterprise means the student understands there is no 'one-size-fits-all' solution to forming a barrier between the malfeasant and the corporate infrastructure. Passing a certification may give the student an edge at obtaining an interview. However, before and after passing a certification, students must be immersed into the world of threat activists and learn from experience and SMEs on how to thwart the malfeasants and protect the enterprise.

In summary, certifications are only one part of the 3-tiered assessment of a student's measure of knowledge. The certification must be balanced with experience and education. Academic programs must match students' cybersecurity problem-solving and theoretical concepts to create a holistic, information security graduate [10]. This necessitates the educator to be a continuous learner, growing with the most current information on the threat landscape, technology changes, governmental regulations, and workforce needs. These qualities of the SME will fulfill the need for cybersecurity experts graduating and moving into the enterprise security community [16]. More importantly, faculty should become certified in their field of expertise to remain current with the technological changes. After obtaining a certification, the faculty can obtain additional training materials from the certifying body to infuse into the curriculum, which provides a way to also improve their current study material [16]. Instructors are permitted the use of pre-packaged instructional materials such as on-line courseware, practice exams, and other assessment tools to aid in classroom instruction [24].

IV. COLLEGE VS CERTIFICATION

As per [15], cybersecurity professionals tend to obtain higher educational degrees than those graduates of traditional computing concentrations, such as software development. According to the survey of the highest education received for cybersecurity professionals, 39% have a bachelor's degree, 43% have a master's degree, 5% attained a doctorate degree [15]. However, is 'certification without education' a quicker means-to-an-end, specifically obtaining employment in the cybersecurity field? Due to financial and time investments required in a college-degree, many people question if the college degree is a worth-while pursuit. The net present value of a college education is less, due to the 4+ years it takes to complete a degree. Many students need the income sooner than 4-years, even though foregoing a degree means less lifetime earnings [17]; as cited by [19]. Also, would only opting for the certification yield the same results in the hiring process? [19] researched data in job openings from Dice.com to determine this answer. Analysis of 11,938 entry-level cybersecurity postings show that 60% of entry-level positions require a college degree in a related IT field, while 24% of those entry-level postings preferred a graduate degree. 29% of the jobs posted required a certification, thereby proving college degrees will promulgate the job applicant to the 'top of the resume stack', and prospective employers are looking for certifications to augment the secondary-education degree.

[24] stated a certification coupled with a post-secondary education creates a stronger theoretical foundation with which to build the hands-on skillset, creating increased marketability in the cybersecurity workforce. Reinforcing that statement, Gigi Escoe, Vice Provost of Undergraduate Studies at the University of Cincinnati [19] stated, students are currently recognizing the value of combining the broad-based foundation of a bachelor's degree with specific skill mastery of industry certifications. Accordingly, a certification coupled with only a high-school degree limits the prospects of employment [24]. Future employers desire the 'holistic' approach by combining the pragmatic with the theory skill sets, or why-you-do-what-you-do. Graduates holding a certification and industry experience will prevail in the job interview process over a high-school graduate with a certification and no experience [24]. The analysis by [19] provided empirical data that college degrees for both bachelor and graduate levels are still in demand for entry-level cybersecurity positions, which asserts the fact that the trend toward degrees and a certification is gaining momentum. While it is possible to for students to obtain cybersecurity certifications through self-study without college curriculum, they will inevitably lack the expertise and real-world experience supplied by the instructor. Hence, memorization of certification questions and answers can become the modus operandi of the student without the supportive reasoning of the instructor.

V. CERTIFICATE VS CERTIFICATION

The difference between certifications and certificates must be distinguished at this juncture in the research paper. Despite the similarity in spelling, the definitions are very different. A certificate is a document stating certain required, academic coursework has been completed in a particular knowledge area. The certificate is normally achieved in shorter period than the degree, and no rigorous exam is given. The coursework may be added to a transcript, with the possibility of credits be applied to a degree. The specifics of the courses encompassed in the certificate and the required passing score is defined by the governing academic institution [28], [8].

A certification is a strenuous exam exhibiting knowledge, ability, and skill of the examinee in a specific knowledge area. The test is governed by industry standards and is independent of an academic institution. While, the exam may encompass both a written and hands-on component, certain certifications mandate some type of classroom education (i.e., the Cisco CCIE). Certifications may be required for professional advancement, and some employers mandate passing a certification before hiring into an enterprise [28],[8].

Certificate	Certification
Governing body is an academic university or college	Governing body is a vendor or professional association
Given in accordance with completion of academic courses as determined by the governing body	Competency exhibit by passing a strenuous exam – can be hands-on skills or written assessment
Can be placed on a transcript	Not part of an academic transcript
Unique to the college administering the certificate	Not part of an academic institution
No industry or professional standardization	Exam questions are set by the industry or vendor
No industry experience necessary	Experience may be necessary before or after taking the exam
Recertification is never necessary	May require periodic recertification

Certificate credits can be used toward a degree	Not related to a IHL degree
Earning a certificate does not mean the person is certified in a particular industry	Typically results in a designation after one's name (i.e., CCNA)
Course credit can be given for past industry experience, in place of taking the course	Certifications are not related to college courses

Table 1. Comparison of the Certificate to the Certification [28], [8].

The first IT certification was recorded in 1989 by Novell, Inc. to determine applicants who had sufficient skills and abilities for the mission critical tasks at Novell [24]. Shortly thereafter, in 1993, Microsoft created the Microsoft Certified Systems Engineer (MCSE) certification, producing approximately150,000 MCSE professionals world-wide [27]. These credentials quickly became the minimum qualification to be hired in the IT workforce in the 1990s. As per [27], Microsoft found that setting a 'benchmark' for competency of the Microsoft products gave employers confidence in the hiring process of candidates. With the influx of newer technologies, e-commerce, and cybersecurity, certifications have been created to showcase knowledge and skillsets of job applicants. Hence, the need to infuse the IHL curriculum with certification material to meet the demand, as per the example of Microsoft in the 1990s.

As defined by [24], "certification is a confirmation of one's adequate knowledge and skills in a specified occupation or occupation specialty" (p. 288). From this definition, two IT certification areas are derived: 1) Vendor-specific - Industry certifications which are geared more toward a particular product, and 2) Vendor-neutral - Professional Association certifications which are issued by organizations. The vendor-specific certifications test skills and knowledge with emphasis on a particular type of hardware (i.e., Cisco Certified Network Administrator, CCNA) and may be viewed by employers as more reflective of current technology. The vendor-specific certification also has shown to be more marketable on a resume [24]. The vendor-neutral certifications test over a broader body of knowledge that does not focus on any hardware or technology vendor (i.e., CompTIA Security+). The vendor-neutral certifications tend to be more flexible, preparing the student for multiple areas of IT by focusing on foundational concepts and theory instead of specific equipment [24].

Vendor-Specific Certification	Vendor-Neutral Certification
Focuses on a vendor's product, service, or technology	Focuses on foundational concepts and job skills- not an underlying technology
Developed and governed by a vendor	Developed and governed by a consortium of experts from industry, public and private sectors
Has industry-wide recognition generally world-wide	Content is designed by a committee from industry and professional associations
Able to prepare curriculum for products before their release, allowing programs to closely match industry trends	Offers an un-biased view and balance for a variety of topics
Information learned by the student does not transfer to another similar technology	Designed to prepare the student for multi-vendor environments and is more well suited for students new to the industry.
Example: Cisco – CCNA – Cisco Certified Network Associate	Example: CompTIA – Security +

Table 2. Comparison of Vendor-Specific and Vendor-Neutral Certification [24]

Certifications to show proficiency and competency in a knowledge area are not a new concept. In health care, law, finance, and even pest control, governing bodies use certifications to assess a candidate's overall capability to use a learned skillset to accomplish a task [16]. As with all certification fields, it is incumbent upon the certification body to assess the current climate and external forces, which will ultimately influence the testing content. This paper discusses three cybersecurity certifying bodies, their background, test domains, and the mapping to the curriculum domains: Amazon Web Services (AWS), CompTIA, and Cisco Certifications. Following this format, other educators can determine which certification is appropriate for their respective curriculum.

VI. SURVEY METHODOLOGY

To better understand the importance of 'education with certification', we applied the mixed method of research, using both qualitative and quantitative studies, as outlined and defined by [6]. In this study, the data collected was from small-to-medium sized businesses within the metro Atlanta area. The companies are focused on diversity, equity, and inclusivity but also aim to empower employees through current training. However, the exact demographic statistics of each company are not available. The survey process included emailing the survey questions to an officer or owner of the company. Surveys completed by the businesses included both a Likert scale questioning system and an open-ended, free response. The free-response question asked to each respondent was: "Overall, what are your thoughts about cybersecurity certifications in academia?" This question was solely developed by the authors and not adopted by prior literature. Appendix A details the responses from the companies.

With the prolific number of certifications available for study, this research focuses on four introductory certifications of: CompTIA Security+, CompTIA Cybersecurity Analyst, Amazon Web Services Certified Cloud Practitioner, Cisco Certified Cisco Network Analyst. The chart below details the certification, governing body, and course content mapping.

Certification	Governing Body	Course Content Mapping
Security +	CompTIA	Operating System Security
CySA+ (Cybersecurity Analyst)	CompTIA	Internet Security
Certified Cloud Practitioner	Amazon Web Services	Cloud Computing Technologies
Certified Cisco Network Analyst	Cisco	Advanced Networks

Table 3: Mapping of certification, Governing Body, and Content Mapping

Reasoning Behind Certification to Course Mapping

To adequately determine the correct certification to course mapping, faculty must have knowledge of three areas: 1) a deep understanding of information contained in the course content and the focus of the different certifications from which to choose, 2) knowledge of the academic level of the students at the college, 3) partnerships with the business community to determine what certifications are requested in a potential new hire [16], [7]. This research focused on these particular certifications, as they are considered by IHLs as introductory certifications, and they mapped to the curriculum content mandated by the University System of Georgia to be taught at the college level for Cybersecurity. Future research may desire to study higher status certifications, such as the Certified Information Systems Security Professional (CISSP).

The results of the Likert Scale Quantitative data received from 12 Information Technology companies in the metro-Atlanta area resulted in the data table in the appendix. The results strongly suggest that certifications in coordination with a college degree propel the graduate into a stronger hiring

position.

VII. RESULTS AND DISCUSSION

See Appendix for Table 4: Showing the results of 12 Information Technology companies in the metro-Atlanta area survey concerning certifications in IHL affecting hiring practices.

The survey results state that >90% of those surveyed agree that a degree that lacks IT certifications make graduates less competitive, >83% state Certifications are important in hiring decisions, 100 % state Multiple IT Certifications gives the employee more confidence in the candidate, 75% state IT certifications are taken into consideration when determining starting salary, and >83% state IT certifications should be embedded into a college degree. These findings can be interpreted to address the conclusion that IT certifications should be incorporated in the IHL curriculum to increase the employment outcomes for graduating students. Furthermore, industry and IHLs must be collaborative partners in the quest to educate students against the current cyber threat and attack forces [25], [24]. By fostering alliances with the local business community, the threat against cybersecurity malfeasants in an organization is reduced with graduates possessing transient, portable IT skills [26]. In working with IHLs to identify a cybersecurity training pathway, local workforce security needs are better met as skills-ready graduates are informed of current the cyber threats in the business community. The National Initiative for Cybersecurity Education [22] created a guidance plan for facilitating the alliance between educational institutes and workforce development in industry which includes the following actions [22]: 1) creation of goals in the alliance, 2) development of implementation strategies, 3) establishment of clear metrics for measurement with each goal, and 4) setting of clear participation expectations from both the IHL and industry.

VIII.PRACTICAL IMPLICATIONS AND FUTURE RECOMMENDATIONS

The business community and industry practitioners are an avid proponent of cybersecurity certifications in IHL education and are seeking talented cybersecurity graduates who have passed certifications, learned the theory supporting security, and have practical hands-on knowledge [15]. Business led activities such as: cyber-range competitions, funding cybersecurity certification fees, and Cyber Patriot Programs, will create a pipeline of graduates into the hiring community. As well, organizations will have a more comprehensive and current knowledge of governmental cybersecurity policies and procedures relevant to their industry over an IHL [21]. In conclusion, partnering IHLs with community businesses will create a shared synergistic vision and bond between education and the enterprise eventuating in a work-place ready college graduate.

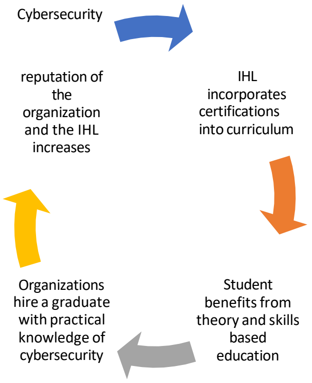
Cybersecurity
reputation of the organization and the IHL increases
IHL incorporates certifications into curriculum
Organizations hire a graduate with practical knowledge of cybersecurity
Student benefits from theory and skills based education

Figure 2: Cyclical Process of Certifications in Curriculum Benefitting both the Student and the Business Community

Recommendations for Future Study

The purpose of this paper is to continue the narrative on the integration of certifications into cybersecurity secondary education based on the present literature. The current study was limited to a sample of small-to-medium sized businesses in the Atlanta, Georgia area, who were recruiting cybersecurity employees. During the research, notice was made that some businesses would hire without a certification but mandated that a certification must be passed within 3-months of employment. Limitations also included using only three certification bodies of CompTIA, AWS, and Cisco. Overcoming these limitations and incorporating the future research topics below would further the study on certifications in the college curriculum.

1. Conduct a curriculum integration study comparing a 2-year college to a 4-year college.
2. Suggested methods to help defray the cost of certifications for students.
3. Efficacy of integrating practice test questions into the curriculum.
4. Package curriculum sources such as TestOut and their preparedness for certifications.
5. Corporate Affiliate Programs (CAPs) -what certifications are most desired.
6. Do certifications increase the ability to receive an internship.
7. Should graduate degrees focus on certifications.
8. How to best decommission certifications.
9. Problems involved with renewing certifications.
10. Upper-level certifications of CISSP, CEH, CIS, CISA, GSED, SSCP and their efficacy in obtaining jobs.
11. Conduct a study to survey what certifications that cybersecurity companies desire on a resume when hiring.

IX. SUMMARY

Educators of cybersecurity are faced with the task of infusing their current curriculum with material that reflects the contemporary cybersecurity threat landscape [24]. Failure in this endeavor reflects on the ill-prepared student as they will lack the knowledge and skills to enter the workforce and be prepared for the battle against cyber criminals. The results of the survey questions from the IT companies show that this deficit in 'education without certification' will jeopardize the organization's critical infrastructure with inadequate risk assessment, critical systems protection, and infrastructure cyberattack. Furthermore, educators of cybersecurity must employ principles of integration of critical thinking and complex problem solving in current threats and breaches. Ultimately, without the necessary cybersecurity preparation in the IHL, including integration of the certification into the curriculum, the threat activist will win, and the organization will suffer both financially and with loss of corporate reputation.

Whereas certifications are not a definitive solution to qualify a student in their cybersecurity field, other qualities, such as hands-on learning, are also a barometer for obtaining the necessary broader interdisciplinary focus of cybersecurity knowledge required for employment. In a wider perspective, certifications can be an indicator of the quality of education being received by the student. Nevertheless, certifications are a gauge of the basic, necessary cybersecurity skills essential for the graduate in the cybersecurity field to which they adopt [2]. It is incumbent upon the Institutes of Higher Learning to continually facilitate student preparation for the workforce. In the realm of cybersecurity, this mandates an integration of certifications into the course curriculum as supported by both the quantitative and qualitative results. One only needs to remember the fact of the hacker only needs to be correct once. The enterprise must be correct every time. If the U.S. is not willing to pivot and produce IHL graduates with certifications and competency which will defend against malfeasant attacks, then it will cease to have a meaningful international presence in the digital world.

REFERENCES

[1] Ackerman, A. (2019). Too few cybersecurity professionals are a gigantic problem. Retrieved https://www.techcrunch.com/2019/01/27/too-few-cybersecurity-professionals-is-a-gigantic-problem-for-2019/

[2] Blažič, B.J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? Educ Inf Technol, 27(1), 3011–3036. doi.org/10.1007/s10639-021-10704-y

[3] Catota, M., Granger, M., Sicker, D., & C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 2(1), 1–19. doi.org/10.1093/cybsec/tyz001

[4] Caulkins, B., Marlow, T., & Reardon, A. (2018). Cybersecurity skills to address today's threats, in Ahram, T. & Nicholson, D., (Eds), Advances in human factors in cybersecurity, AHFE 2018. Advances in Intelligent Systems and Computing, 1, 782-788. Springer. doi.org/10.1007/978-3-319-94782-2-2_18

[5] Coker, J. (2022). Cybersecurity workforce gap grows by 26% in 2022. Infosecurity Magazine. Retrieved from https://www.infosecurity-magazine.com/news/cybersecurity-workforce-gap-grows

[6] Creswell, J.W. (2009). Qualitative, Quantitative, and Mixed Methods Approaches. (3rd ed.). Sage.

[7] Davri, E. C., Darra, E., Monogioudis, I., Grigoriadis, A., Iliou, C., Mengidis, N., ... & Farah, M. A. B. (2021, July). Cyber Security certification programmes. In 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 428-435). IEEE. Retrieved from https://pure.port.ac.uk/ws/files/42722324/Cyber_Security_Certification_Programmes.pdf

[8] Dennon, A. (2021). Certificates vs. certifications vs. licenses. Best Colleges. Retrieved from https://www.bestcolleges.com/blog/certificates-certifications-licenses/

[9] Elzey, K. & Jyotishi, S.R. (2020). Combining degrees with quality certifications is a win for everyone. RealClear Education. Retrieved from https://www.realcleareducation.com/articles/2020/07/01/combining_degrees_with_quality_certifications_is_a_win_for_everyone_110439.html

[10] Erickson, M., & Kim, P. (2021). Designing cybersecurity curriculum: Exploring the need for industry certifications and experiential learning. Issues in Information Systems. 22(4), 9-20. doi.org/10.4.48009/4_iis_2021_9-21

[11] GIAC.org. (2020). The value of certifications. GIAC Certifications. Retrieved from https://www.giac.org/blog/the-value-of-certifications/

[12] Hallett, J., Larson, R., & Rashid, A. (2018). Mirror, mirror, on the wall: What are we teaching them all? Characterizing the focus of cybersecurity curricular frameworks. In 2018 USENIX Workshop on Advances in Security Education (ASE 18). International Information System Security Certification. Retrieved from https://www.usenix.org/system/files/conference/ase18/ase18-paper_hallett.pdf

[13] Harris, M.A., Patten, K.P. (2015). Using Bloom's and Webb's taxonomies to integrate emerging cybersecurity topics into a computing curriculum. Journal of Information Systems Education. 26(3), 219-214. Retrieved from https://aisel.aisnet.org/jise/vol26/iss3/4/

[14] Hentea, M., Dhillon, H. S., & Manpreet, D. (2006). Towards changes in information security education. International Journal of IT Education, 5, 221-233. Retrieved from https://www.semanticscholar.org/paper/Towards-Changes-in-Information-Security-Education-Hentea-Dhillon/24d546fd424566a70f41bf77b60bbcf62da0da50

[15] ISC2. (2022). 2022 Cybersecurity workforce study: The cybersecurity workplace evolves as staff shortages grow. Retrieved from https://www.isc2.org/Research/Workforce-Study#

[16] Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. Journal of Information Systems Education, 28(2), 101-114. Retrieved from http://jise.org/Volume28/n2/JISEv28n2p101.html

[17] Lobo, B. J., & Burke-Smalley, L. A. (2018). An empirical investigation of the financial value of a college degree. Education Economics, 26(1), 78–92. doi.org/10.1080/09645292.2017.13 32167

[18] Locasto, M. E., Ghosh, A. K., Jajodia, S., & Stavrou, A. (2011). The ephemeral legion: producing an expert cyber-security work force from thin air. Communications of the ACM, 54(1), 129-131. doi:10.1145/1866739.1866764

[19] Marquardson, J., & Elnoshokaty, A. (2020). Skills, certifications, or degrees: What companies demand for entry-level cybersecurity jobs. Information Systems Education Journal, 18(1), 22-28. Retrieved from https://eric.ed.gov/?id=EJ1246234

[20] Morgan, S. (2020). The 2019/2020 Official Annual Cybersecurity Jobs Report. Herjavec Group. Retrieved from https://www.herjavecgroup.com/wp-content/uploads/2019/10/HG-CV-2019-Cybersecurity-JobsReport.pdf

[21] National Workforce Centers for Emerging Technologies. (2003). Building a foundation for tomorrow: Skill standards for information technology. Bellevue, WA.

[22] NICE Program Office (2016). National Initiative of Cybersecurity Education (NICE) strategic plan. Retrieved from https://www.nist.gov/document/nicestrategicplan011218webpdf

[23] Powell, O. (2022). The biggest data breaches and leaks of 2022. Cybersecurity Hub. Retrieved from https://www.cshub.com/attacks/articles/the-biggest-data-breaches-and-leaks-of-2022#

[24] Randall, M.H. & Zirkle, C.J. (2005). Information Technology student-based certification in formal education settings:Who benefits and what is needed. Journal of Information Technology Education: Research, 4(1), 287-306. Informing Science Institute. Retrieved from https://www.learntechlib.org/p/111576/

[25] Rybnicek, R., Königsgruber, R. (2019). What makes industry–university collaboration succeed? A systematic review of the literature. Journal of Business Economics, 89, 221–250. doi.org/10.1007/s11573-018-0916-6

[26] Santos, D., Santos, D., Goel, S., Costanzo, J., Sagen, D., & Buddelmeyer, P. (2020). A roadmap for successful regional alliances and multistakeholder partnerships to build the cybersecurity workforce. US Department of Commerce, National Institute of Standards and Technology. doi.org/10.6028/NISST.IR.8287

[27] Siddiqui, Y. (2018). The history of Microsoft certifications. QuickStart. Retrieved from https://quickstart.com/blog/the-history-of-microsoft-certifications

[28] University of Virginia. (2022). Certificate vs. certification. School of Continuing and Professional Studies. Retrieved from https://www.scps.virginia.edu/certificate-vs-certification

[29] U.S. Department of Labor, Bureau of Labor Statistics. (2021). Why computer occupations are behind strong STEM employment growth in the 2019-29 decade. Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6

[30] U.S. Department of Labor, Bureau of Labor Statistics. (2018). Cybersecurity consultant: Career Outlook. Retrieved from https://www.bls.gov/careeroutlook/2018/interview/cybersecurity-consultant.htm

APPENDIX

Table 4: Showing the results of 12 IT companies in the metro-Atlanta area survey concerning certifications in IHL affecting hiring practices from section VII.

12 Information Technology Companies	Strong Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)	Results
1. A degree that lacks IT certifications make graduates less competitive	0	0	1	3	8	> 90%
2. Certifications are important in hiring decisions	0	1	1	3	7	>83%
3. Multiple IT Certifications gives the employee more confidence in the candidate	0	0	0	2	10	100%
4. IT Certifications are taken into consideration when determining starting salary	0	0	3	6	3	75%
5. IT Certifications should be embedded into a college degree	0	1	1	5	5	>83%

The following table represents the qualitative responses from an open-ended survey question to businesses concerning implementation of certifications into college curriculum. The free-response question asked was:

Overall, what are your thoughts about IT Certifications in Academia?

The table below summarizes the answers from the businesses surveyed:

1. IT Certifications are a MUST during these competitive market times, so students should be prepared to have them as part of their formal education.
2. A candidate that does not have IT certifications results in more theoretical knowledge and can be harder to train.
3. IT Certifications should be added to all degrees so graduates are more workforce ready.
4. IT Certifications alone are not enough but if complemented with a degree offers students substantial advantage.
5. The right IT certifications must be taken to show employers that they are able to learn rapidly and independently.
6. Certifications create a balance between theory and hands-on knowledge making graduates more employable.
7. Students should strive to have 1 or more certifications to make them stand out.
8. Certifications are absolutely essential for hiring and also can lead to a higher starting salary.
9. Colleges and universities need to graduate students who are ready to enter the workforce with minimal training.
10. It is important to know that certifications alone are not enough but added with a degree is very advantages.
11. Depending on the position, the right certifications can be very beneficial from a hiring standpoint.
12. I do not see any disadvantages to having IT certifications along with a degree to make the candidate stronger in the job market.