Environmental Scan:

Undergraduate Programming in Cybersecurity

Kugel University

Submission by:

UPCEA

Center for Research and Strategy

January 2021

Data and names have been changed for the illustrative use/purpose of this report

Table of Contents

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

I. Program Overview

Kugel University (KU) is interested in offering a cybersecurity certificate and/or undergraduate degree. The curriculum would focus on three distinct areas in which the University has already established courses and resources including business, criminal justice, and information technology management courses. Repackaging and combining existing coursework should help control cost associated with program development. KU is pursuing more aggressively pursuing veteran recruitment, which it believes would promote greater interest in cybersecurity programming. The program(s) would be delivered online and on-campus.

II. Objective

Kugel University has requested the University Professional and Continuing Education Association (UPCEA) and its Center for Research and Strategy to provide information concerning the current market for potential programming in Cybersecurity. The University would like greater information on the potential market and its size, curriculum topics, and the competitive environment.

The goal of this environmental scanning effort is to answer the following questions:

- What is the condition of the market for a program in cybersecurity?
- What would employer demand potentially be for this degree and/or certificate?
- Is there information available that could impact content development or course offerings?
- What is the size, magnitude, delivery method, and cost of the competition?
- Do a certificate and degree have equal demand in the cybersecurity marketplace?

Environmental scanning is a cost-efficient and insightful exploratory research method regarding program assessment, design, and delivery—an internal stakeholder engagement and planning adaptation enabler. It rarely provides a conclusive Go/No-Go decision.

III. Methodology

UPCEA and its Center for Research and Strategy conducted an environmental scan that included a review of cybersecurity trends, occupational demographics, and internet and library scans. This report presents occupational and demographic information for three regions: [redacted] as the primary region; the states of North Dakota, South Dakota, Iowa, Illinois, and Wisconsin as the secondary region; and the United States as the tertiary region. For this research, nine cybersecurity-related occupations were selected: information security analysts; computer and information systems managers; network and computer systems administrators; computer systems analysts; computer network architects; computer programmers; computer network support specialists; computer user support specialists; and database administrators and architects.

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

IV. Key Findings

Occupational Analysis

- The current occupational outlook is more favorable nationally than it is in the primary and secondary regions for the select occupations. The 10-year forecasted growth rate for these occupations is 11% nationally, well above the percentages of both the secondary region (5%) and primary region (3%). Information security analysts is forecasted to see the greatest growth across all three regions.

- The typical entry-level education for the majority of select cybersecurity occupations is a bachelor's degree. In job postings, the percentage mentioning a bachelor's degree ranges from [redacted] 48% to 51% nationally.

- Computer systems analysts has the highest number of jobs in the primary and secondary regions, while computer user support specialists employs the highest number of professionals nationally.

- Among job postings for select cybersecurity occupations in the United States from October 2019 to October 2020, Oracle Corporation had the highest number of unique postings at 50,473, followed by Robert Half International Inc. (28,367) and General Dynamics Corporation (19,639). The Army National Guard had the highest posting intensity.

- Between October 2019 and October 2020, the top cities in terms of unique job postings for select cybersecurity professionals were New York, NY (68,452), followed by Washington, DC (52,363), and Atlanta, GA (37,478). Charlotte, NC had the highest posting intensity of 8:1. The top cities in the primary region were City A (14,722) and City B (4,762).

- Computer user support specialists and computer systems analysts were two of the top three occupations by unique job postings posted in each region.

- Computer science and SQL (programming language) were two of the top three in-demand skills among all job postings for select cybersecurity occupations. Other critical skills include operating systems, automation, and agile methodology.

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Competitive Analysis

- According to the Integrated Postsecondary Education Data System (IPEDS), national completions in computer and information systems security programs among all credential levels have increased each year since 2003. Since 2012, distance offered programs have increased 296% from 2,499 completions to 9,907 in 2019.

- Nationally, bachelor's-level completions in computer and information systems security have increased steadily from 5,397 in 2010, to 17,652 in 2019.

- UPCEA conducted research on 12 competitors who offer bachelor's degrees in cyber-security-related fields. Three of these competitors are located in [redacted]. Four institutions offer their programs online. In addition, one institution offers its program in a hybrid model. The average annual tuition for a [redacted] resident is $24,406. For comparison, Kugel's annual undergraduate tuition is $10,438.

- Among bachelor's degree programs, the most common subject areas include network security (12), programming languages (9), and cybersecurity technologies (8).

- UPCEA also researched 10 other institutions which offer undergraduate certificates in cybersecurity-related fields. Two of these competitors are located in [redacted]. One offers its program online and the other provides a hybrid delivery. The average tuition for a [redacted] resident is $8,160.

- All of the 10 undergraduate certificate programs in cybersecurity offer comprehensive curriculum on network security and cybersecurity technologies. Machine learning is the least covered topic area, as none of the profiled institutions offer a course in this area.

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

V. Recommendations

The following recommendations were shaped by the data generated by a review of the occupational and competitive marketplaces, and an understanding of the current and projected trends within the cybersecurity industry. Recommendations are included to help aid program development and add value to the program and should not be considered definitive or absolute. Recommendations are not listed by priority or importance.

- Cautiously Move Forward with Program Development: While the marketplace for bachelor's degree programs in cybersecurity is becoming increasingly competitive, there may still be room for entry into the field, particularly for a program that is priced below some competing institutions and offers unique qualities. Additionally, the University should move forward with the undergraduate certificate offering as it will be able to repackage and combine existing coursework which should reduce the cost and time associated with program development. Each program's viability will depend on multiple factors including how the program is marketed, the ability to maintain a modern and relevant curriculum in a field that updates frequently, and the success and failures of competing programs, among others.

- Maintain an In-State Focus During Initial Launch: Should the University move forward with program development, it should consider maintaining an in-state focus during the initial launch. Currently, there are four institutions within the state that offer bachelor's degree programming, few of which have the resources and brand recognition that KU enjoys. While occupational growth within the state is somewhat limited, the University's brand strength will likely make it an immediate player in the [redacted] market. Focusing marketing and development in-state and expanding out into the region will help concentrate marketing and recruitment resources.

- Attempt to Capture [Competitor Name Redacted] Current Market Share Through Price Conscious Marketing and Alumni Connections: [Redacted competitor] accounted for 28.5% (51 students) of all computer and information systems security bachelor's degree completions in [redacted] in 2019. [Redacted competitor] current annual undergraduate tuition for in-state residents is $14,450, well above Kugel's $10,438. Emphasizing the affordability to price-conscious students through marketing efforts could be particularly appealing in the wake of the pandemic where there is less money for education. Additionally, the University could highlight the size and success of its alumni in the field, adding yet another layer of value.

- Pursue an Online Delivery: In order to attract students from major metropolitan areas such as Minneapolis, Chicago, and Milwaukee, and to more effectively compete against online programs such as [redacted competitor], the University should pursue an online delivery. This online delivery will also help facilitate the University's ability to attract military veterans.

UPCEA
©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

- As One Audience Among Others, Target and Prioritize Veterans: Due to the defense-oriented nature of cybersecurity, and Kugel's previously stated commitment to veteran recruitment, the University should target and prioritize veterans. They could potentially be a unique element of the program, which would aid visibility in the competitive marketplace.

- Develop, Isolate, and Market Unique Qualities of the Program: Because Kugel University will be competing with other in-state and online institutions for a limited number of students, the University will need to develop, isolate, and market the unique qualities of the bachelor's degree and undergraduate certificate programs. If the University decides to pursue a standalone bachelor's degree, it could explore the potential of specializations such as financial cybersecurity, data security, and healthcare cybersecurity.

- Consider Additional Research: The University should consider conducting additional research through a survey of potential students or interviews of industry professionals. Potential students could be asked about their interest in the program, their preferred delivery method, brand strength, and price sensitivity. Obtaining this data would allow for a more accurate estimated market size and would aid program performance measurements and internal planning processes. Additionally, speaking to industry professionals would allow the University to better align the curriculum with industry needs. Obtaining guidance from outside professionals could create additional interest in the program as they may be likely to have their employees enroll in the program.

UPCEA

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

VI. Trends in Cybersecurity

AI's Increasing Role in Cyber-Attacks and Defense

Behavioral Detection

Artificial intelligence development is becoming increasingly leveraged across the world. It can be used to attack an enemy state's civil and defense infrastructure or be utilized by criminal gangs and terrorist organizations. AI is continuously improving and updating to account for new forms of cyberattacks and defense. For example, behavioral detection using machine learning is viewed by industry experts as one of the best software solutions for defense-in-depth cybersecurity. It works by monitoring network activity to provide a baseline of normal behavior, and then uses that baseline to check for abnormal behavior. However, while this tool is used for defense, it can also be reverse engineered by cyber terrorists. In 2019 Instagram suffered two cybersecurity attacks and it has been hypothesized that hackers used AI systems to scan Instagram user data for potential vulnerabilities.[1]

Vulnerabilities of the Internet of Things

Current IoT Flaws

As a broader range of devices becomes equipped to connect to the internet, it becomes easier for cybercriminals to bypass network security by targeting the endpoint device with the weakest security.[2] The Internet of things (IoT) has expanded to include devices such as coffee makers, lights, thermostats, ovens, laundry machines, and yoga mats which creates more potential vulnerabilities. One of the most significant IoT vulnerabilities is that owners rarely change the factory default usernames and passwords which can be found online, in catalogs, or by purchasing the same device. Similarly, there is often a lag between the time when critical software patches are released and when they are downloaded by device owners, allowing cybercriminals time to continue exploiting glitches and faulty programming for weeks or months after the problem has been made public and corrected by the device manufacturer. [3]

[1] https://www.infoq.com/articles/ai-cyber-attacks/
[2] https://www.csoonline.com/article/3241242/cybersecurity-trends-to-watch.html
[3] https://www.networkworld.com/article/3332032/top-10-iot-vulnerabilities.html

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Cybersecurity Talent Gap

Careers in Cybersecurity

The combination of continuous advancements in technology, increases in cybersecurity threats, and regulatory changes have all led to strong demand for cybersecurity professionals. These factors also provide a reason for organizations to invest in their existing staff. Cybersecurity professionals are needed across industries, in both the public and private sectors, to protect organizations from malicious threats.[4] Most affected by potential cybersecurity staffing shortages are the educational, financial, governmental, healthcare, manufacturing, online retail, and transportation industries.[5] Projections by Cisco pointed to a global shortage of two million cybersecurity professionals by the end of 2019.[6] According to a New York Times report, Cybersecurity Ventures estimated that by 2021 there would be 3.5M unfilled cybersecurity jobs globally, one million more than in 2014.[7]

Effects of the Talent Gap

One immediate ramification of the talent shortage is that 54% of companies are working with external security consultants, and 47% are outsourcing incident response. Outsourcing these security services allows existing employees to focus on strategic initiatives, rather than spending all their time reacting to problems.[8] A second effect of the talent gap is that companies may lack depth among their cybersecurity professionals. Cybersecurity encompasses a broad range of technical skills, and organizations facing talent gaps will have weaknesses in their security protocols. Lastly, employers are not sure how to identify qualified applicants.[9] The field is not fully established yet, and employers struggle to clearly define job qualifications and responsibilities.[10]

[4] https://www.redteamsecure.com/the-top-6-industries-at-risk-for-cyber-attacks/
[5] https://www.globalsign.com/en/blog/top-industries-preparing-for-evolving-cybersecurity-threats/
[6] https://gblogs.cisco.com/ch-tech/closing-the-cyber-security-talent-gap/Trends
[7] https://cybersecurityventures.com/jobs/
[8] https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf
[9] https://www.secureworldexpo.com/industry-news/impacts-of-cybersecurity-talent-shortage-gap
[10] https://www.isc2.org/-/media/Files/Research/ISC2-Hiring-and-Retaining-Top-Cybersecurity-Talent.ashx

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

VII. Occupational and Demographic Analysis

For this research, nine cybersecurity-related occupations were selected: information security analysts; computer and information systems managers; network and computer systems administrators; computer systems analysts; computer network architects; computer programmers; computer network support specialists; computer user support specialists; and database administrators and architects. While these are not the only occupations that could benefit from the program, they provide valuable insight into the overall market while demonstrating potential career paths for professionals with a bachelor's degree or certificate.

This report presents occupational and demographic information for three regions: [redacted] as the primary region; the states of North Dakota, South Dakota, Iowa, Illinois, and Wisconsin as the secondary region; and the United States as the tertiary region. All data is presented from Economic Modeling Specialists International (Emsi) and its 2020.4 data set.

Primary Region

Table 1 details the current and forecasted occupational data for select cybersecurity occupations in [redacted]. Over the next 10 years, the nine occupations are expected to see an average 3% increase, with information security analysts having the highest growth at 23% and computer programmers having the lowest at -10%. Computer systems analysts currently has the greatest number of jobs (21,286), about 6,000 more than the next highest and the most annual openings.

Table 1: Current and Forecasted Occupational Data for Select Cybersecurity-Related Occupations in [Redacted]

Occupation	Number of Jobs in Field		10-Year Predicted Job Growth		Median Annual Salary	Annual Openings*	Typical Entry-Level Education
	2020	2030	# of Jobs	% Change			
Computer and Information Systems Managers	10,937	11,613	676	6%	$141,127	960	Bachelor's degree
Computer Network Architects	2,943	2,949	6	0%	$113,666	218	Bachelor's degree
Computer Network Support Specialists	4,705	4,841	136	3%	$63,150	415	Associate's degree
Computer Programmers	4,776	4,317	-459	-10%	$82,288	326	Bachelor's degree
Computer Systems Analysts	21,286	21,631	345	2%	$92,473	1,619	Bachelor's degree
Computer User Support Specialists	14,703	15,638	935	6%	$55,404	1,362	Some college, no degree
Database Administrators and Architects	2,797	2,942	145	5%	$98,213	222	Bachelor's degree
Information Security Analysts	2,391	2,943	552	23%	$101,419	246	Bachelor's degree
Network and Computer Systems Administrators	6,813	6,959	146	2%	$84,281	512	Bachelor's degree
Total	**71,352**	**73,833**	**2,481**	**3%**		**5,881**	

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

*Annual Openings: Annual openings is an estimated employment change and turnover for an occupation for a given year. Openings are a combination of two types of data:

1. Job Growth: An employer experiences a greater demand for its products and hires new employees to increase production. If job growth is zero or negative, all openings are due to replacement needs.
2. Replacement Needs: An employer hires replacement workers for employees who leave the workforce or change occupations. Replacement rates are derived from national 10-year, occupation-specific percentages published by the Bureau of Labor Statistics Employment Projections (EP) program.

Figure 1 gives an overview of select cybersecurity occupations in the primary region. There are 71,352 jobs in [redacted], 18% higher than the national average for a comparable workforce size or the national average adjusted for region size. The median annual compensation for the select occupations in the region is $85,982, which is greater than the adjusted national average. The monthly job posting demand is on par with the adjusted national average.

Figure 1: Occupation Summary - Primary Region

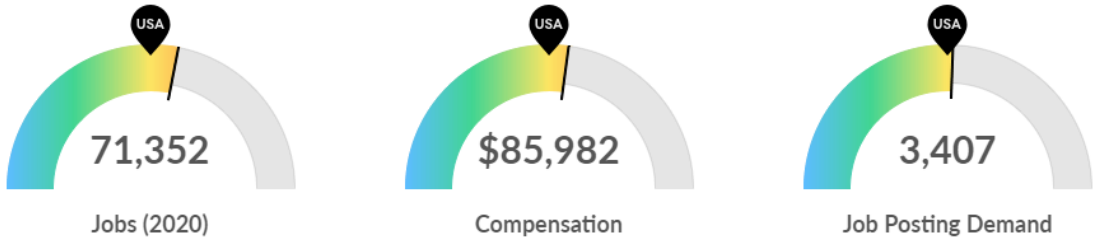


Table 2 shows that eight of the top 10 counties in [Redacted] are predicted to see growth over the next decade in the number of select cybersecurity occupations. The largest percentage is predicted in County G (10%), and the greatest change by number will likely occur in County A (1,250 jobs).

Table 2: Current and Forecasted Occupational Data for Select Cybersecurity-Related Occupations in [Redacted] by County

County	2020 Jobs	2030 Jobs	2020 – 2030 Change	2020 – 2030 % Change	Median Annual Salary	Annual Openings
County A	35,930	37,180	1,250	3%	$93,258	2,912
County B	9,938	9,384	-554	-6%	$89,498	734
County C	5,019	5,181	162	3%	$81,010	406
County D	2,323	2,473	150	6%	$79,157	199
County E	1,661	1,781	120	7%	$79,072	143
County F	1,297	1,260	-37	-3%	$75,630	99
County G	1,146	1,258	112	10%	$63,827	107
County H	1,135	1,163	28	2%	$68,295	93
County I	914	955	41	6%	$81,431	77
County J	856	904	48	6%	$82,826	72

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Figure 2 shows the job posting intensity for the select occupations in [redacted]. There were 204,219 total job postings from October 2019 to October 2020, of which 43,103 were unique. This results in a posting intensity of 5:1, meaning that for every five postings, there is one unique job posting. This is slightly higher than the posting intensity average for all other occupations in the state (4:1), indicating that companies are putting in an above-average effort to hire cybersecurity professionals. There was a median posting duration of 32 days, which is one day less than the regional average.

Figure 2: Job Posting Intensity for Select Cybersecurity-Related Occupations in [Redacted]

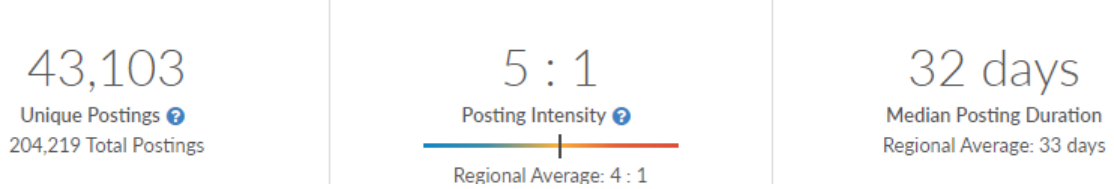


Figure 3 lists education and experience levels, whether preferred, required, or negotiable, in job postings from October 2019 to October 2020 in the primary region for the select occupations. The most common education level was a bachelor's degree (48%), with the next closest being high school or GED (10%). It should be noted that 41% of the unique postings did not specify an education level requirement. Over half of the postings (35%) did not list any experience. Of those that did, 26% required 2-3 years, and another 17% required 0-1 years.

Figure 3: Education and Experience Breakdown in Select Job Postings – Primary Region

Education Level	Unique Postings	% of Total
Unspecified	17,810	41%
High school or GED	4,241	10%
Associate's degree	3,435	8%
Bachelor's degree	20,772	48%
Master's degree	3,738	9%
Ph.D. or professional degree	258	1%

Minimum Experience	Unique Postings	% of Total
No experience listed	15,009	35%
0 - 1 Years	7,240	17%
2 - 3 Years	11,342	26%
4 - 6 Years	6,954	16%
7 - 9 Years	1,706	4%
10+ Years	852	2%

Figure 4 shows the top 10 cities in the primary region by number of job postings for select the occupations. City A had the most total and unique postings from October 2019 to October 2020, including 14,772 unique postings, followed by City B (4,762) and City C (1,943). City G had the highest posting intensity at 7:1, followed by City C at 6:1.

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Figure 4: Top Cities Posting in the Primary Region for Select Cybersecurity-Related Occupations

City	Total/Unique (Oct 2019 - Oct 2020)	Posting Intensity	Median Posting Duration
City A	79,799 / 14,772	5 : 1	36 days
City B	22,783 / 4,762	5 : 1	31 days
City C	12,127 / 1,943	6 : 1	32 days
City D	5,947 / 1,495	4 : 1	35 days
City E	6,340 / 1,190	5 : 1	37 days
City F	5,818 / 1,179	5 : 1	32 days
City G	5,762 / 774	7 : 1	43 days
City H	3,373 / 770	4 : 1	35 days
City I	3,461 / 632	5 : 1	35 days
City J	2,866 / 615	5 : 1	32 days

Figure 5 ranks the top companies in [Redacted] by number of unique job postings for the select occupations. Wells Fargo & Company had the most total and most unique postings from October 2019 to October 2020, including 2,807 unique postings, followed by the Oracle Corporation (1,187), and UnitedHealth Group Incorporated (907). UnitedHealth Group had the highest posting intensity of 8:1.

Figure 5: Top Companies Posting in the Primary Region for Select Cybersecurity-Related Occupations

Company	Total/Unique (Oct 2019 - Oct 2020)	Posting Intensity	Median Posting Duration
Wells Fargo & Company	20,460 / 2,807	7 : 1	15 days
Oracle Corporation	6,154 / 1,187	5 : 1	44 days
UnitedHealth Group Incorporated	6,959 / 907	8 : 1	27 days
Robert Half International Inc.	3,280 / 730	4 : 1	24 days
International Business Machines Corporation (IBM)	4,663 / 688	7 : 1	40 days
U.S. Bancorp	4,335 / 651	7 : 1	40 days
Apex Systems, Inc.	2,462 / 485	5 : 1	36 days
Genesis10	2,777 / 414	7 : 1	35 days
Target Corporation	1,689 / 397	4 : 1	18 days
Deloitte LLP	1,983 / 387	5 : 1	57 days

Figure 6 on the following page lists the 10 most common job titles by number of unique job postings for the select occupations. Business systems analysts had the most unique postings from October 2019 to October 2020, with 617 unique posts, followed by information security engineers (515) and data entry specialists (429). Information security engineers and application systems engineers had the highest posting intensity at 7:1.

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Figure 6: Top Job Titles in the Primary Region for Select Cybersecurity-Related Occupations

Job Title	Total/Unique (Oct 2019 - Oct 2020)	Posting Intensity	Median Posting Duration
Business Systems Analysts	3,142 / 617	5 : 1	31 days
Information Security Engineers	3,568 / 515	7 : 1	17 days
Data Entry Specialists	1,642 / 429	4 : 1	27 days
Network Engineers	2,104 / 416	5 : 1	34 days
Systems Administrators	1,575 / 365	4 : 1	33 days
IT Specialists	1,732 / 331	5 : 1	35 days
Business Systems Consultants	1,637 / 266	6 : 1	15 days
Information Security Analysts	1,341 / 253	5 : 1	23 days
Application Systems Engineers	1,579 / 235	7 : 1	14 days
Technical Support Representatives	1,206 / 222	5 : 1	42 days

Figure 7 shows the nine select occupations' job postings from October 2019 to October 2020, with computer user support specialists having the most total (54,726) and unique (11,655) postings. All the occupations have a posting intensity equal to or higher than the regional average for all occupations.

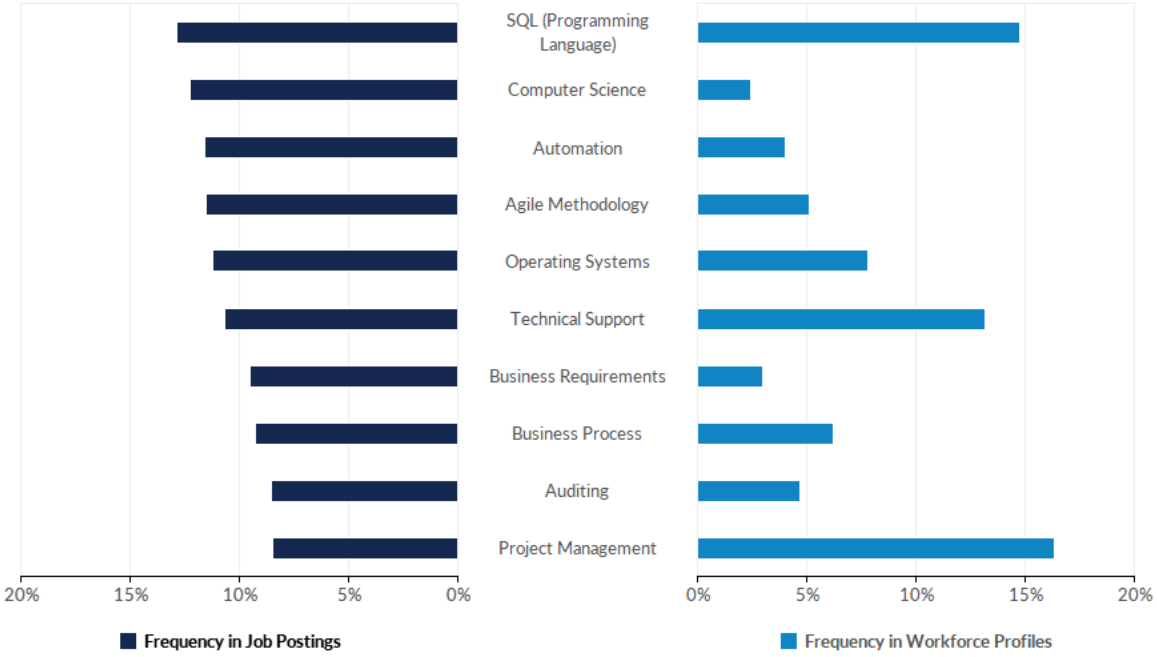
Figure 7: Top Posted Occupations – Primary Region

Occupation (SOC)	Total/Unique (Oct 2019 - Oct 2020)	Posting Intensity	Median Posting Duration
Computer User Support Specialists	54,726 / 11,655	5 : 1	32 days
Computer Systems Analysts	50,054 / 10,081	5 : 1	32 days
Network and Computer Systems Administrators	31,914 / 7,110	4 : 1	32 days
Information Security Analysts	25,148 / 4,930	5 : 1	30 days
Computer and Information Systems Managers	22,669 / 4,542	5 : 1	34 days
Computer Programmers	10,716 / 2,562	4 : 1	29 days
Database Administrators and Architects	6,093 / 1,564	4 : 1	27 days
Computer Network Architects	2,053 / 510	4 : 1	32 days
Computer Network Support Specialists	846 / 149	6 : 1	33 days

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Figure 8 illustrates the top hard skills in job postings and workforce profiles from October 2019 to October 2020 in the primary region for select occupations. Employers were most often looking for hard skills in SQL (programming language) (13%), while 15% of workforce profiles reported having this skill. Computer science, automation, and agile methodology were the next most frequent hard skills in job postings at approximately 12%.

Figure 8: Top Hard Skills in Job Postings and Workforce Profiles – Primary Region



©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Secondary Region

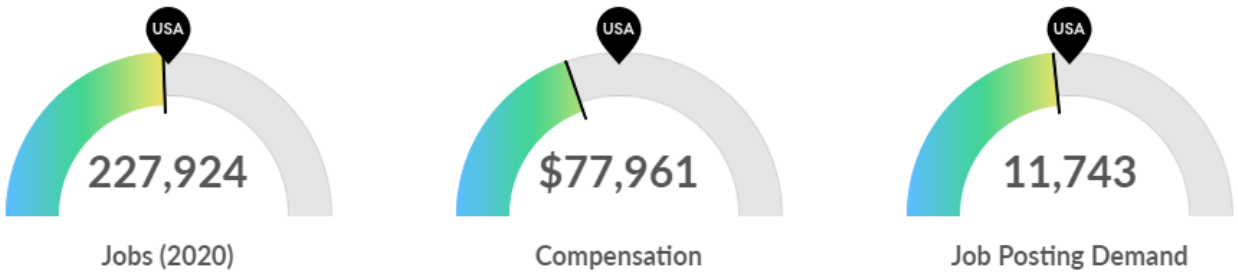
Table 3 highlights the current and forecasted occupational data for select cybersecurity-related occupations in the secondary region. Over the next 10 years, computer programmers is the only occupation expected to decrease (-8%). Computer systems analysts (56,377) has the most jobs, followed by computer user support specialists (50,298). Computer user support specialists are projected to have the highest job growth (4,110) by 2030, with almost 2,000 more than the next highest.

Table 3: Current and Forecasted Occupational Data for Select Cybersecurity-Related Occupations in the Secondary Region

Occupation	Number of Jobs in Field		10-Year Predicted Job Growth		Median Annual Salary	Annual Openings*	Typical Entry-Level Education
	2020	2030	# of Jobs	% Change			
Computer and Information Systems Managers	33,087	35,472	2,385	7%	$133,349	2,940	Bachelor's degree
Computer Network Architects	9,165	9,404	239	3%	$111,212	702	Bachelor's degree
Computer Network Support Specialists	19,746	20,103	357	2%	$59,887	1,726	Associate's degree
Computer Programmers	18,989	17,445	-1,544	-8%	$80,740	1,321	Bachelor's degree
Computer Systems Analysts	56,377	58,438	2,061	4%	$84,842	4,434	Bachelor's degree
Computer User Support Specialists	50,298	54,408	4,110	8%	$49,200	4,756	Some college, no degree
Database Administrators and Architects	7,906	8,503	597	8%	$94,002	652	Bachelor's degree
Information Security Analysts	7,340	9,035	1,695	23%	$94,184	754	Bachelor's degree
Network and Computer Systems Administrators	25,016	25,715	699	3%	$76,029	1,897	Bachelor's degree
Total	**227,924**	**238,523**	**10,599**	**5%**		**19,181**	

Figure 9 gives an overview of the select cybersecurity-related occupations in the secondary region. There are 227,924 jobs in the secondary region, which is 4% lower than the adjusted national average of 235,349. The median annual compensation for the select occupations is $77,961, less than the adjusted national average. The monthly job posting demand is slightly below the adjusted national average.

Figure 9: Occupation Summary - Secondary Region



©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Figure 10 outlines the job posting intensity for select cybersecurity-related occupations in the secondary region from October 2019 to October 2020. There were 737,580 total job postings, of which 144,930 were unique, a posting intensity of 5:1. The median posting duration was 35 days.

Figure 10: Job Posting Intensity for Select Cybersecurity-Related Occupations in the Secondary Region

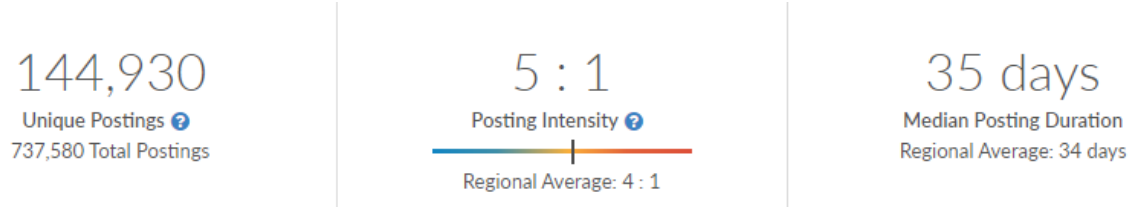


Figure 11 gives education and experience levels in job postings from October 2019 to October 2020 in the secondary region for the select occupations. The most common education level was a bachelor's degree (49%), followed by a high school diploma or GED and a master's degree, both at 9%. It should be noted that 40% of the unique postings did not specify an education level requirement. Thirty-eight percent of the postings did not list experience. Of those that did, 24% require 2-3 years and another 16% 4-6 years of experience.

Figure 11: Education and Experience Breakdown in Select Job Postings – Secondary Region

Education Level	Unique Postings	% of Total
Unspecified	58,617	40%
High school or GED	13,706	9%
Associate's degree	11,196	8%
Bachelor's degree	71,317	49%
Master's degree	12,542	9%
Ph.D. or professional degree	1,435	1%

Minimum Experience	Unique Postings	% of Total
No experience listed	55,230	38%
0 - 1 Years	22,233	15%
2 - 3 Years	35,498	24%
4 - 6 Years	23,020	16%
7 - 9 Years	5,656	4%
10+ Years	3,293	2%

Figure 12 on the following page lists the top 10 cities in the secondary region by number of job postings for the select occupations. Chicago, IL, had the most total and unique (37,055) postings from October 2019 to October 2020, followed by Milwaukee, WI (6,908), and Madison, WI (5,868). Six cities had a posting intensity at 6:1.

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Figure 12: Top Cities Posting in the Secondary Region for Select Cybersecurity-Related Occupations

City	Total/Unique (Oct 2019 - Oct 2020)	Posting Intensity	Median Posting Duration
Chicago, IL	205,948 / 37,055	6 : 1	43 days
Milwaukee, WI	36,177 / 6,908	5 : 1	35 days
Madison, WI	34,220 / 5,868	6 : 1	34 days
Des Moines, IA	23,764 / 4,538	5 : 1	33 days
Schaumburg, IL	11,652 / 1,840	6 : 1	33 days
Deerfield, IL	10,308 / 1,773	6 : 1	35 days
Sioux Falls, SD	9,825 / 1,765	6 : 1	42 days
Fargo, ND	8,649 / 1,719	5 : 1	40 days
Springfield, IL	7,087 / 1,673	4 : 1	25 days
Cedar Rapids, IA	9,204 / 1,509	6 : 1	38 days

Figure 13 ranks the top companies across the secondary region by number of unique job postings for the select occupations. Oracle Corporation had the most unique (2,934) postings from October 2019 to October 2020, followed by Wells Fargo & Company (2,529), and Robert Half International Inc. (2,417). The Army National Guard had the highest posting intensity, 15:1.

Figure 13: Top Companies Posting in the Secondary Region for Select Cybersecurity-Related Occupations

Company	Total/Unique (Oct 2019 - Oct 2020)	Posting Intensity	Median Posting Duration
Oracle Corporation	16,865 / 2,934	6 : 1	46 days
Wells Fargo & Company	14,677 / 2,529	6 : 1	12 days
Robert Half International Inc.	13,820 / 2,417	6 : 1	33 days
Army National Guard	22,185 / 1,512	15 : 1	57 days
Teksystems, Inc.	10,737 / 1,229	9 : 1	31 days
Apex Systems, Inc.	7,903 / 1,214	7 : 1	40 days
Revature	8,298 / 1,171	7 : 1	31 days
Computer Task Group, Incorporated	3,393 / 1,169	3 : 1	32 days
Deloitte LLP	6,631 / 1,066	6 : 1	47 days
Humana Inc.	5,855 / 987	6 : 1	39 days

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Figure 14 lists the 10 most common job titles by number of unique job postings for the select occupations. Network engineers had the most unique (1,685) postings from October 2019 to October 2020, followed by systems administrators (1,621), and business systems analysts (1,283). IT specialists had the highest posting intensity ratio, 7:1.

Figure 14: Top Job Titles in the Secondary Region for Select Cybersecurity-Related Occupations

Job Title	Total/Unique (Oct 2019 - Oct 2020)	Posting Intensity	Median Posting Duration
Network Engineers	7,758 / 1,685	5 : 1	35 days
Systems Administrators	7,627 / 1,621	5 : 1	37 days
Business Systems Analysts	7,024 / 1,283	5 : 1	32 days
IT Specialists	9,190 / 1,252	7 : 1	46 days
.NET Developers	4,392 / 910	5 : 1	34 days
Data Entry Specialists	3,363 / 857	4 : 1	30 days
Database Administrators	3,890 / 826	5 : 1	37 days
Information Security Engineers	4,549 / 782	6 : 1	22 days
Senior Network Engineers	3,818 / 682	6 : 1	35 days
Help Desk Analysts	3,478 / 672	5 : 1	34 days

Figure 15 shows the nine select occupations' job postings from October 2019 to October 2020, with computer user support specialists having the most total (196,418) and unique (39,140) postings. All the posting intensities are equal to or higher than the regional average for all occupations.

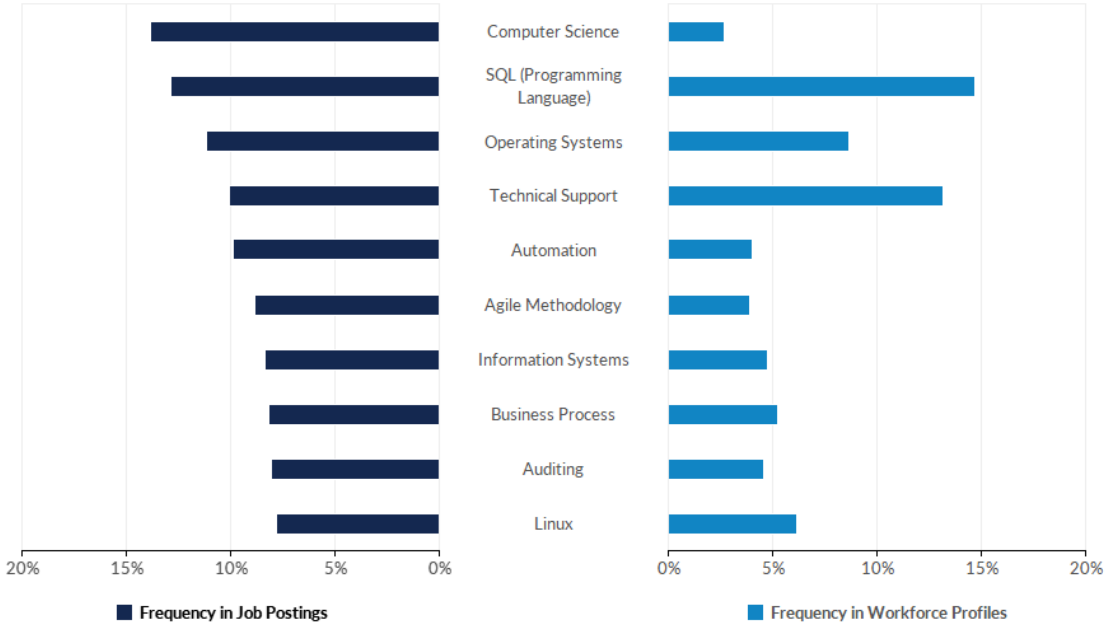
Figure 15: Top Posted Occupations – Secondary Region

Occupation (SOC)	Total/Unique (Oct 2019 - Oct 2020)	Posting Intensity	Median Posting Duration
Computer User Support Specialists	196,418 / 39,140	5 : 1	36 days
Computer Systems Analysts	157,930 / 30,266	5 : 1	34 days
Network and Computer Systems Administrators	127,499 / 25,963	5 : 1	35 days
Computer and Information Systems Managers	86,879 / 16,362	5 : 1	37 days
Information Security Analysts	84,286 / 15,722	5 : 1	33 days
Computer Programmers	47,062 / 9,727	5 : 1	31 days
Database Administrators and Architects	24,424 / 5,162	5 : 1	32 days
Computer Network Architects	9,158 / 1,956	5 : 1	33 days
Computer Network Support Specialists	3,924 / 632	6 : 1	38 days

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Figure 16 illustrates the top hard skills in job postings and workforce profiles in the secondary region from October 2019 to October 2020 for the select occupations. Employers were most often looking for hard skills in computer science (14%), but only 3% of workforce profiles reported having this as a skill. The next most frequently listed were SQL (programming language) (13%) and operating systems (11%).

Figure 16: Top Hard Skills in Job Postings and Workforce Profiles– Secondary Region



©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Tertiary Region

Table 4 details the current and forecasted occupational data for the select cybersecurity-related occupations in the United States. Over the next 10 years, the number of computer programmers is expected to decrease by 2%. The other occupations are predicted to increase by 7-28%. Computer and information systems managers, as in the other regions, has the highest median salary ($143,901).

Table 4: Current and Forecasted Occupational Data for Select Cybersecurity-Related Occupations in the United States

Occupation	Number of Jobs in Field		10-Year Predicted Job Growth		Median Annual Salary	Annual Openings*	Typical Entry-Level Education
	2020	2030	# of Jobs	% Change			
Computer and Information Systems Managers	481,289	544,442	63,153	13%	$143,901	46,721	Bachelor's degree
Computer Network Architects	160,510	171,725	11,215	7%	$111,787	13,136	Bachelor's degree
Computer Network Support Specialists	215,024	234,288	19,264	9%	$63,383	20,703	Associate's degree
Computer Programmers	260,399	255,056	-5,343	-2%	$82,786	19,213	Bachelor's degree
Computer Systems Analysts	667,337	733,972	66,635	10%	$90,284	57,912	Bachelor's degree
Computer User Support Specialists	777,931	877,827	99,896	13%	$52,174	78,595	Some college, no degree
Database Administrators and Architects	133,759	149,513	15,754	12%	$92,997	11,753	Bachelor's degree
Information Security Analysts	134,534	172,657	38,123	28%	$99,733	14,781	Bachelor's degree
Network and Computer Systems Administrators	376,239	404,343	28,104	7%	$82,627	30,673	Bachelor's degree
Total	**3,207,023**	**3,543,824**	**336,801**	**11%**		**293,486**	

Figure 17 gives an overview of select cybersecurity-related occupations in the United States. There are currently 3,207,023 jobs for the select occupations across the nation. The average compensation is $82,556, and the monthly job posting demand is 176,092.

Figure 17: Occupation Summary - Tertiary Region

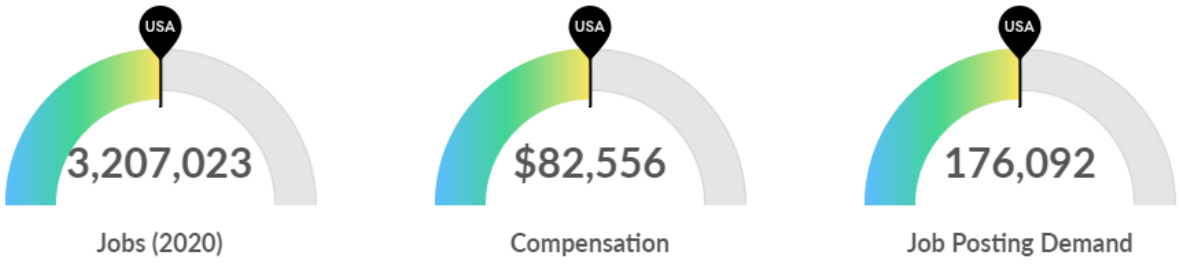


Figure 18 on the following page outlines the job posting intensity for select cybersecurity occupations in the United States between October 2019 to October 2020. During that time, there were 11.6 million total job postings, of which 2.18M were unique, a posting intensity of 5:1. The median posting duration for the select occupations was 35 days.

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Figure 18: Job Posting Intensity for Select Cybersecurity-Related Occupations in the Tertiary Region

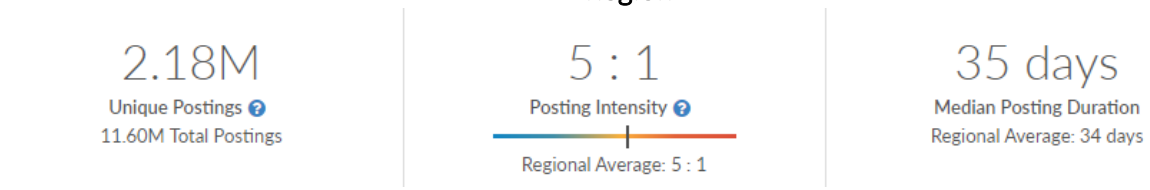


Figure 19 lists education and experience levels, whether preferred, required, or negotiable, in job postings from October 2019 to October 2020 in the tertiary region for the select occupations. The most common education level was a bachelor's degree (51%), followed by a master's degree (10%). It should be noted that 40% of the unique postings did not specify an education level requirement. Thirty-seven percent did not list a required experience; of those that did, the most common experience requirements were 2-3 years (24%) and 4-6 years (18%).

Figure 19: Education and Experience Breakdown in Select Job Postings – Tertiary Region

Education Level	Unique Postings	% of Total
Unspecified	868,408	40%
High school or GED	203,255	9%
Associate's degree	142,233	7%
Bachelor's degree	1,107,307	51%
Master's degree	219,349	10%
Ph.D. or professional degree	36,450	2%

Minimum Experience	Unique Postings	% of Total
No experience listed	796,667	37%
0 - 1 Years	306,313	14%
2 - 3 Years	525,531	24%
4 - 6 Years	388,420	18%
7 - 9 Years	101,809	5%
10+ Years	62,314	3%

Figure 20 on the next page shows the top 10 cities in the United States by number of job postings for select cybersecurity occupations. New York, NY had the most total and unique postings from October 2019 to October 2020, including 68,452 unique postings, followed by Washington, DC (52,363), and Atlanta, GA (37,478). Charlotte, NC has the highest posting intensity of 8:1.

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Figure 20: Top Cities Posting in the Tertiary Region for Select Cybersecurity-Related Occupations

City	Total/Unique (Oct 2019 - Oct 2020)	Posting Intensity	Median Posting Duration
New York, NY	437,882 / 68,452	6 : 1	36 days
Washington, DC	256,166 / 52,363	5 : 1	36 days
Atlanta, GA	215,847 / 37,478	6 : 1	39 days
Chicago, IL	205,948 / 37,055	6 : 1	43 days
San Francisco, CA	144,883 / 26,698	5 : 1	39 days
Dallas, TX	138,154 / 26,121	5 : 1	39 days
Houston, TX	139,949 / 24,520	6 : 1	35 days
Los Angeles, CA	116,849 / 24,170	5 : 1	34 days
Austin, TX	143,140 / 23,812	6 : 1	45 days
Charlotte, NC	166,461 / 21,979	8 : 1	45 days

Figure 21 shows the top companies across the tertiary region by number of job postings for select cybersecurity-related occupations. Oracle Corporation had the most total and unique postings from October 2019 to October 2020, including 50,473 unique postings, followed by Robert Half International Inc. (28,367) and General Dynamics Corporation (19,639). The Army National Guard had the highest posting intensity of 15:1. Nine had a posting intensity higher than the regional average for all occupations.

Figure 21: Top Companies Posting in the Tertiary Region for Select Cybersecurity-Related Occupations

Company	Total/Unique (Oct 2019 - Oct 2020)	Posting Intensity	Median Posting Duration
Oracle Corporation	281,231 / 50,473	6 : 1	48 days
Robert Half International Inc.	181,730 / 28,367	6 : 1	31 days
General Dynamics Corporation	194,507 / 19,639	10 : 1	58 days
Wells Fargo & Company	135,444 / 19,349	7 : 1	15 days
Deloitte LLP	120,427 / 18,717	6 : 1	50 days
Leidos Holdings, Inc.	193,358 / 18,066	11 : 1	45 days
Army National Guard	232,439 / 15,790	15 : 1	56 days
International Business Machines Corporation (IBM)	116,491 / 15,529	8 : 1	40 days
Kforce Inc.	106,313 / 14,995	7 : 1	43 days
Computer Task Group, Incorporated	42,875 / 14,408	3 : 1	31 days

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Figure 22 lists the top 10 most common job titles by the number of job postings for the select occupations in the United States. Network engineers had the most total and unique postings from October 2019 to October 2020, including 28,997 unique posts, followed by systems administrators (28,977), and business systems analysts (18,110). IT Specialists had the highest posting intensity ratio at 7:1.

Figure 22: Top Job Titles in the Tertiary Region for Select Cybersecurity-Related Occupations

Job Title	Total/Unique (Oct 2019 - Oct 2020)	Posting Intensity	Median Posting Duration
Network Engineers	160,722 / 28,997	6 : 1	36 days
Systems Administrators	155,607 / 28,977	5 : 1	36 days
Business Systems Analysts	107,219 / 18,110	6 : 1	34 days
IT Specialists	123,102 / 17,714	7 : 1	40 days
Database Administrators	69,982 / 12,861	5 : 1	38 days
.NET Developers	55,127 / 11,940	5 : 1	31 days
Senior Network Engineers	64,027 / 11,806	5 : 1	37 days
Security Engineers	61,313 / 10,984	6 : 1	38 days
Systems Engineers	60,995 / 10,363	6 : 1	39 days
Network Administrators	48,873 / 9,957	5 : 1	37 days

Figure 23 shows the nine select occupations' job postings from October 2019 through October 2020, with computer user support specialists having the most at total (2,868,033) and unique (522,023) job postings, with a posting intensity of 5:1.

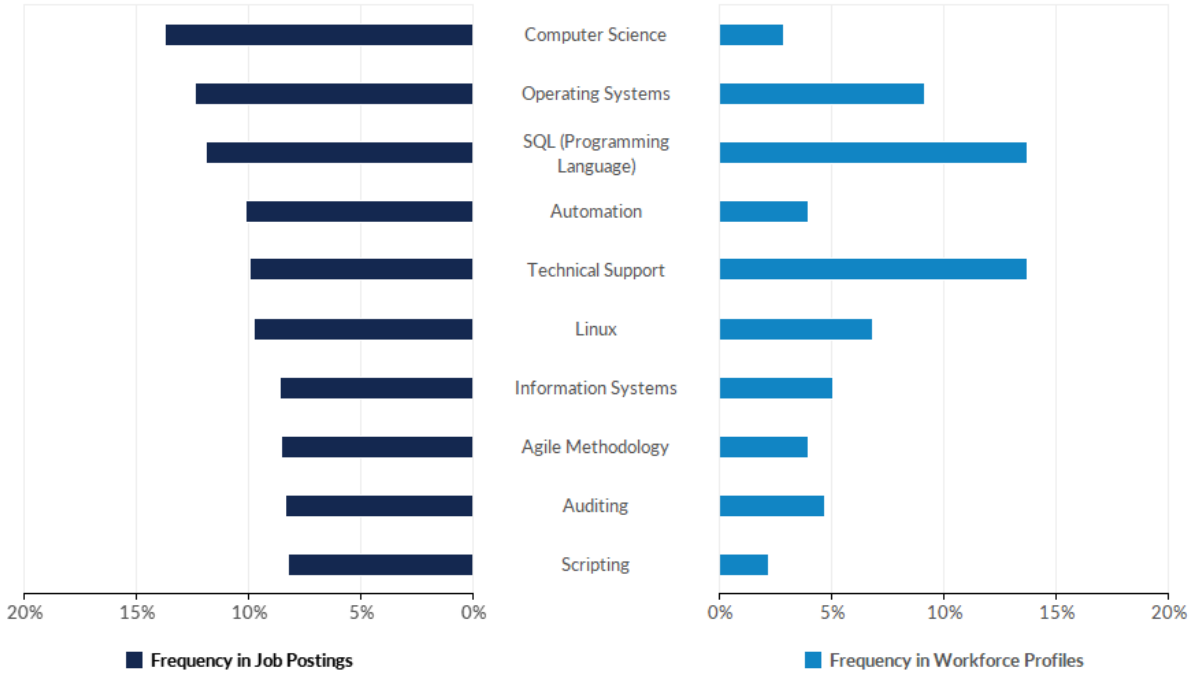
Figure 23: Top Posted Occupations – Tertiary Region

Occupation (SOC)	Total/Unique (Oct 2019 - Oct 2020)	Posting Intensity	Median Posting Duration
Computer User Support Specialists	2,868,033 / 552,023	5 : 1	35 days
Network and Computer Systems Administrators	2,356,726 / 444,027	5 : 1	35 days
Computer Systems Analysts	2,238,624 / 415,234	5 : 1	35 days
Information Security Analysts	1,672,439 / 289,775	6 : 1	37 days
Computer and Information Systems Managers	1,244,085 / 235,835	5 : 1	36 days
Computer Programmers	631,084 / 127,329	5 : 1	30 days
Database Administrators and Architects	381,304 / 77,980	5 : 1	32 days
Computer Network Architects	161,818 / 30,876	5 : 1	35 days
Computer Network Support Specialists	42,285 / 7,975	5 : 1	34 days

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Figure 24 illustrates the top hard skills in job postings and workforce profiles in the tertiary region from October 2019 to October 2020 for the select occupations. Employers were most often looking for hard skills in computer science (14%), but only 3% of workforce profiles reported having this as a skill. Following computer science, job postings most frequently listed operating systems) (12%) and SQL (programming language) (12%).

Figure 24: Top Hard Skills in Job Postings and Workforce Profiles– Tertiary Region



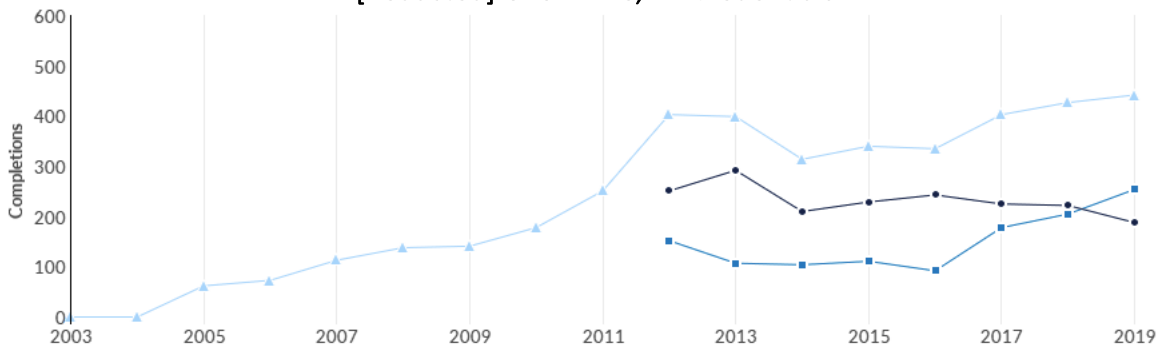
©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

VIII. Competitive Analysis

The programs featured in the following competitive analysis do not constitute an exhaustive list of competitors but rather provide an overall representation of the current marketplace. Because tuition costs are often estimated and routinely do not include additional fees, the tuition prices should be used more as guidelines rather than definitive bounds. For programs that do not post a set total tuition, either a per-credit rate or annual rate was used to calculate the tuition for a full-time student. Additional information about each competing program is available in Appendix I.

Figure 25 shows the number of Computer and Information Systems Security (CIP 11.1003) program completions among all credential levels over time in [Redacted]. Total completions had increased from 62 in 2005 to 442 in 2019. IPEDS began tracking distance completions of all programs in 2012. Distance-offered program completions are defined as "a program for which all the required coursework can be completed via distance education courses. All completions of this program are considered distance-offered completions, even if some students chose not to enroll in distance education courses."[11] This means that if there are 10 distance-offered completions, and four of these were completed online and six completed on campus, all 10 would be counted as distance-offered completions. From 2012 to 2019, distance-offered completions decreased by 25%. Completions data is taken from the national IPEDS database published by the U.S. Department of Education's National Center for Education Statistics.

Figure 25: Computer and Information Systems Security Program Completions in [Redacted] Over Time, All Credentials



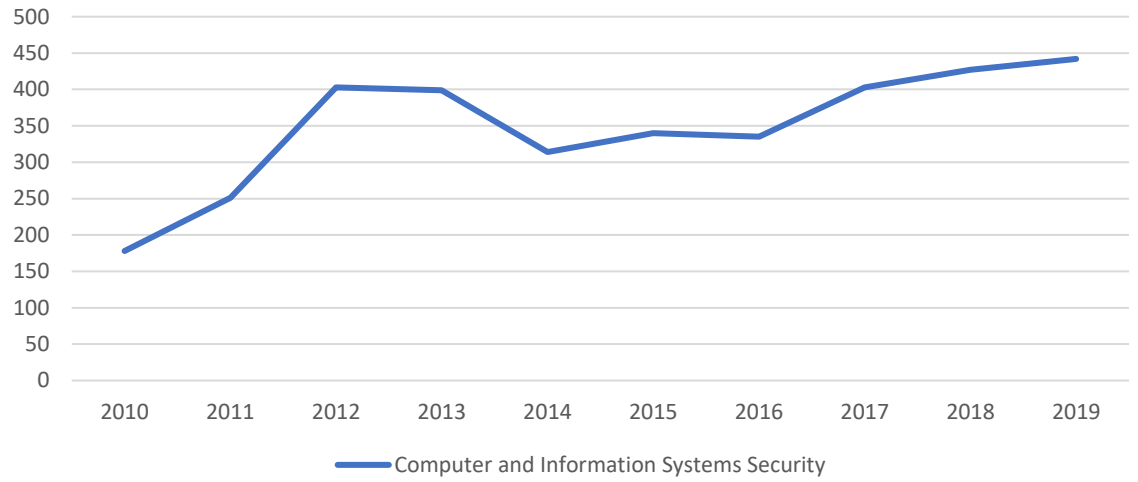
	2012 Completions	2019 Completions	% Change
Distance Offered Programs	251	188	-25.1%
Non-Distance Offered Programs	152	254	+67.1%
All Programs	403	442	+9.7%

[11] https://www.economicmodeling.com/2017/11/20/emsi-introduces-data-related-distance-offered-academic-programs/

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

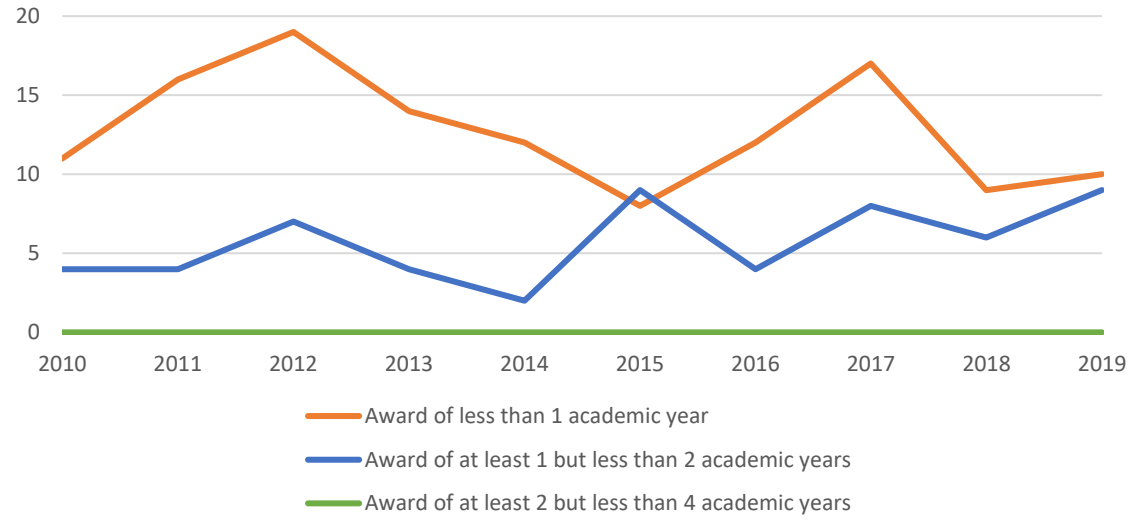
Figure 26 shows computer and information systems security completions at the bachelor's level between 2010 and 2019 in [redacted]. Completions have risen steadily aside from a drop in 2014 but overall increasing from 178 in 2010 to 442 in 2019.

Figure 26: Computer and Information Systems Security
Bachelor's Degree Completions 2010-2019 in [Redacted]



Figures 27 shows computer and information systems security completions in [redacted] at the certificate level broken out into their sub-categories between 2010 and 2019. Awards of less than one academic year had the most completions each year from 2010 to 2019 except for 2015.

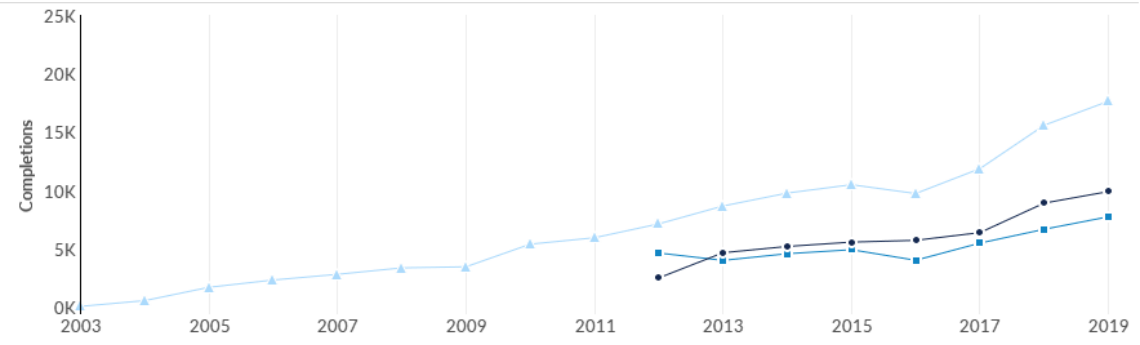
Figure 27: Computer and Information Systems Security
Certificate Completions 2010-2019 in [Redacted]



©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Figure 28 shows the number of Computer and Information Systems Security program completions among all credential levels over time on a national scale. Total completions increased from 62 in 2003 to 17,652 in 2019 and grew every year except in 2016. Non-distance programs increased by 3,107 completions from 2012 to 2019 but had drop-offs in 2013 and 2016. From 2012 to 2019, distance-offered completions increased by 7,408, almost 300%.

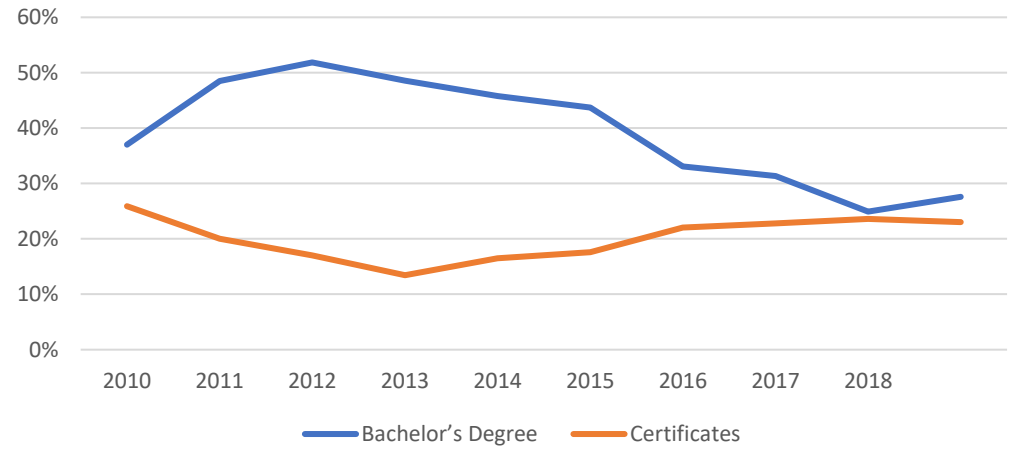
Figure 28: Computer and Information Systems Security Program Completions in the United States 2010-2019, All Credentials



	2012 Completions	2019 Completions	% Change
Distance Offered Programs	2,499	9,907	+296.4%
Non-Distance Offered Programs	4,638	7,745	+67.0%
All Programs	7,137	17,652	+147.3%

Figure 29 illustrates the percentage of all computer and information systems security completions at the bachelor's degree and certificate levels. Bachelor's degrees accounted for 37% of all completions in 2010 and increased to a high of 52% in 2012. Since then, they have fallen to just under 30% in 2019 and hit a low of 24% in 2018. Certificates were highest in 2010, fell to 13% in 2013, and climbed back up to 24% in 2019.

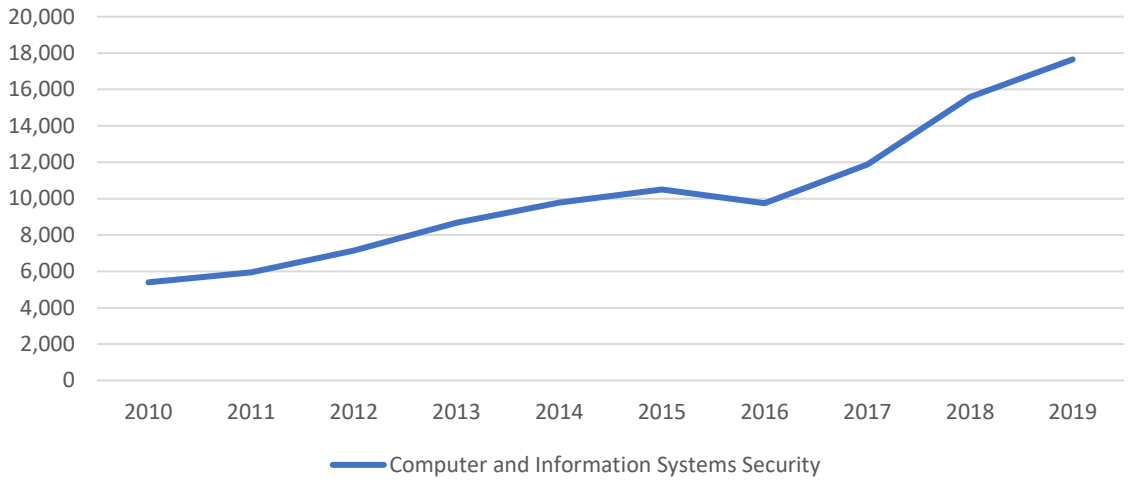
Figure 29: Computer and Information Systems Security Program Completions in the United States, Bachelor's Degrees and Certificates as a Percentage of Overall Completions



©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

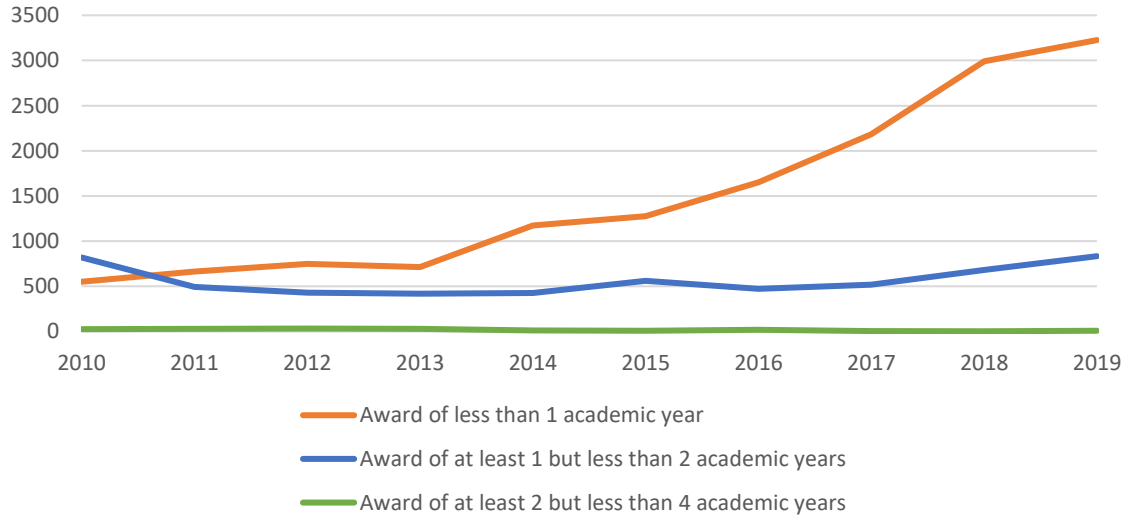
Figures 30 shows computer and information systems security completions at the bachelor's level between 2010 and 2019. Bachelor's completions have risen steadily with only a slight drop off in 2016, but increasing from almost 5,400 in 2010 to 17,652 in 2019.

Figure 30: Computer and Information Systems Security
Bachelor's Degree Completions 2010-2019 in the United States



Figures 31 shows computer and information systems security completions at the certificate level broken out into their sub-categories between 2010 and 2019. Awards of at least one but less than two academic years had the most completions in 2010 but were surpassed by awards of less than one academic year in 2011. Awards of less than one academic year have steadily grown over the years from 511 completions in 2010 to 3,226 in 2019, while awards of at least one but less than two academic years and awards of at least two but less than four academic years have changed from 2010 to 2019.

Figure 31: Computer and Information Systems Security
Certificate Completions 2010-2019 in the United States



©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Table 5 lists 10 potential competing institutions in the United States that offer cybersecurity certificates. Only Institution D offers its program online. The average total tuition among the featured programs for residents of [redacted] is $8,160. Institution J has the highest out-of-state tuition at $32,300 and Institution B, the lowest ($2,500).

Table 5: Potential Competitors for Computer and Information Systems Security Certificates

Institution	Location	Program Name	Delivery	Length	Tuition for Full Program	
					In-State	Out-of-State
Institution A	Pewaukee, WI	Cyber Security Specialist Certificate	On-Campus	20 Credits	$2,778	$4,167
		Security Administrator Certificate		17 Credits	$2,361	$3,541
Institution B	Fond Du Lac, WI	Information Technology – Information Security Certificate	On-Campus	12 Credits	$1,666	$2,500
Institution C	Inver Grove Heights, MN	Certificate in Network/Information Security	On-Campus	15 Credits	$2,529	
Institution D	Duluth, MN	Cyber Defense Certificate	Online and On-Campus	30 Credits	$7,000	
		Cyber Security Certificate		18 Credits	$4,000	
Institution E	Rockford, IL	Cisco CCNA Security Certificate/3776	Hybrid	10 Credits	$2,930	$5,490
		Cisco CCNA Security Certificate/3777		18 Credits	$5,274	$9,882
Institution F	Bloomfield Hills, MI	Computer Information Systems – Cybersecurity Certificate (CIS.CYS.CT)	On-Campus	36 Credits	$3,492	$6,768
Institution G	Calmar, IA	Certificate in Information Security	On-Campus	21 Credits	$4,200	$4,704
Institution H	Palos Hills, IL	Network Security Specialist, Certificate	On-Campus	36 Credits	$4,716	$13,320
Institution I	Crystal Lake, IL	Cyber Security Certificate	On-Campus	21 Credits	$2,342.00	$9,873
Institution J	Ankeny, IA	Digital Forensic Investigation Certificate	On-Campus	19 Credits	$32,300	

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Figure 32 illustrates 2019 bachelor's degree completions in computer and information security in [Redacted]. Institution K (51.4%) had the most completions in 2019.

Figure 32: [Redacted] Institution's Bachelor's Degree Completions in Computer and Information Systems Security

Institution	Bachelor's Degree Completions (2019)	Growth % YOY (2019)	Market Share (2019)
Institution K	92	73.6%	51.4%
Institution L	51	-10.5%	28.5%
Institution Q	30	30.4%	16.8%
Institution X	6	-45.5%	3.4%

Table 6 lists 12 potential competitor institutions in the Midwest that offer a bachelor's degree in cybersecurity. Four offer their programs online, three of which also offer their programs on-campus. The average in-state tuition is $24,406. For comparison, Kugel's annual undergraduate tuition is $10,438.

Table 6: Potential Competitors for Computer and Information Systems Security Bachelor's Degrees

Institution	Location	Program Name	Delivery	Length	Tuition per Year	
					In-State	Out-of-State
Institution K	St. Cloud, MN	Bachelor of Science in Cybersecurity	On-Campus	78 Credits	$8,890	$17,432[12]
Institution L	Minneapolis, MN	Bachelor of Science in Information Technology – Information Assurance and Cybersecurity Specialization	Online	180 Quarter Credits	$14,450	
Institution M	Menomonie, WI	Bachelor of Science in Applied Mathematics and Computer Science – Cyber Security Concentration	On-Campus	120 credits	$9,488	$17,455
Institution O	Madison, SD	Cyber Operations (BS)	Online and On-Campus	120 credits	$ 16,683	$ 19,754
Institution P	Chicago, IL	Applied Cybersecurity and Information Technology (B.S.)	On-Campus	129 credits	$48,670	
Institution Q	Saint Paul, MN	Bachelor of Science in Cybersecurity Computer Forensics (BAS)	On-Campus	120 credits	$7,030	$14,344
Institution R	Chicago, IL	Bachelor of Science in Computer Science – Computer Networks and Security concentration	On-Campus	120 credits	$12,366	$24,732
Institution S	Chicago, IL	Bachelor of Science in Cyber and Information Security	On-Campus	120 credits	$31,493	
Institution T	Dubuque, IA	Bachelor of Science in Computer Forensics & Security	Hybrid	120 credits	$34,070	
Institution U	Champaign, IL	Bachelor of Science in Computer Science (Engineering) – Illinois Cyber Security Scholars Program	On-Campus	120 credits	$21,956	$39,406
Institution V	Springfield, IL	Information Systems Security Bachelor's Degree	Online and On-Campus	120 credits	$8,670	$18,127
Institution W	West Lafayette, IN	Cybersecurity, BS	Online and On-Campus	120 credits	$9,992	$28,794

[12] Tuition rate changes depending upon the state of residence of the student. The listed tuition is for "all other non-residents."

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Table 7 is a curriculum heat map of topics offered by 10 institutions delivering cybersecurity certificates. All have courses in network security, 9 offer courses in cyber security technologies, and 8 have courses in cyber forensics. However, none offer courses in machine learning, and only 4 offer ethics.

Table 7: Competitive Curriculum for Computer and Information Systems Security Certificates

Institution	Network Security	Machine Learning	Programming Languages	Cyber Security Technologies	Cyber Forensics	Ethics
Institution B						
Institution C						
Institution D						
Institution E						
Institution F						
Institution G						
Institution H						
Institution I						
Institution J						

Key: Comprehensive curriculum: Related or partial curriculum: No offering:

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Table 8 shows a curriculum heat map of topics offered by institutions delivering bachelor's degrees in computer and information systems security. All 12 offer courses in network security, and 10 have courses in programming languages. Only one offers machine learning.

Table 8: Competitive Curriculum Heatmap for Computer and Information Systems Security Bachelor's Degrees

Institution	Network Security	Machine Learning	Programming Languages	Cyber Security Technologies	Cyber Forensics	Ethics
Institution K						
Institution L						
Institution M						
Institution O						
Institution P						
Institution Q						
Institution R						
Institution S						
Institution T						
Institution U						
Institution V						
Institution W						

Key: Comprehensive curriculum: Related or partial curriculum: No offering:

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Appendix I

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

The following information was taken from each institution's website.

Cybersecurity Certificates

Institution A — *Cyber Security Specialist Certificate & Security Administrator Certificate*

Institution A's Cyber Security Specialist Certificate is a 63-credit program. In which students expand their skills through service-learning projects, emerging technology exploration, and global business technology. The Security Administrator Certificate is a 17-credit program where students experience hands-on experience in configuring network operating systems, firewalls, VPNs, packet filters and intrusion detection systems.

Institution B — *Information Technology – Information Security Certificate*

Institution B's Information Security Certificate is a 12-credit program in which students learn about implementation techniques to maintain information security, gain skills to respond to compromised networks and vulnerabilities, and identifying intrusion methods, policy development, encryption and authentication.

Institution C — *Certificate in Network/Information Security*

Institution C offers a 15-credit certificate in Network Security. Students learn about security incident management, Cisco, IOS and ASA firewalls, ethical hacking, VPNS, and intrusion detection.

Institution D — *Cyber Defense Certificate & Cyber Security Certificate*

Institution D's Cyber Defense Certificate is a 30-credit certificate program. Students learn how to manage Cisco router hardware and the Cisco Internet Operating System, analyze organization network needs and implement networks, describe and identify common security threats and attacks. It's designed to prepare students for a career in computer networking and security. The Cyber Security certificate is 18-credits and is designed for students with prior computer or networking experience and prepares them for the EC-Council Certified Ethical Hacker (CEH) certification.

Institution E — *Cisco CCNA Security Certificate/3776 & Cisco CCNA Security Certificate/3777*

Institution E offers a 10 credit Cisco CCNA Security Certificate/3776 where students learn how network security relates to other areas of information technology, network design, security policy design, Cisco and ASA firewall design. The Cisco CNNA Security Certificate/3777 is an 18-credit certificate that includes all of the courses in the 3776 certificate and adds two classes in which students will learn about VLANs, spanning tree protocol, redundant links, Hot Standby Router Protocol, troubleshooting, routing solutions, and converged networks.

UPCEA
©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Institution F — *Computer Information Systems – Cybersecurity Certificate (CIS.CYS.CT)*

Institution F's Computer Information Systems – Cybersecurity Certificate fosters knowledge of software risks, database systems and security, breach of security and privacy, and computer security. Students will learn how to detect potential attacks from hackers and defenses against them and also learn computer ethics.

Institution G — *Certificate in Information Security*

Institution G offers a 21-credit certificate in Information Security. The program prepares students to enter the workforce as an information security analyst, network administrator, security architect, network and/or web penetration tester. Students will learn computer ethics, structured program design, effective control the operation, identifying intrusions, implementation of safeguards, and have hands-on experience with building, monitoring, and troubleshooting home or small business networks.

Institution H — *Network Security Specialist, Certificate*

Institution H's Network Security Specialist certificate develops students' skills in preserving confidential information, risk management, and data integrity, availability and authenticity. Students will also sharpen their firewall, VPN and data assurance knowledge to be prepared to work as specialists in the workforce.

Institution I — *Cyber Security Certificate*

Institution I offers a 21-credit Cyber Security Certificate where students learn security skills to apply in the workforce. Credits earned in this certificate can be applied toward a student's Network Security AAS or Help Desk Technician AAS.

Institution J — *Digital Forensic Investigation Certificate*

Institution J offers a 19-credit Digital Forensic Investigation Certificate that concentrates in data recovery and digital forensics. Areas of study include diving into evidence analysis, specifically networked environments, and portable data storage/communication devices. Students should be interested in careers in law enforcement, corrections, and security.

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Cybersecurity bachelor's degree:

Institution L— *Bachelor of Science in Information Security – Information Assurance and Cyber Security Specialization*

Institution L's Bachelor of Science in Information Security with a Specialization in Information Assurance and Cyber Security is offered fully online and aims to fill in the skills gap in the field of cybersecurity. The skills acquired prepare students to play an important role in the infrastructure that supports commerce, banking, telecommunications, healthcare, and national security.

Institution K — *Bachelor of Science in Cyber Security*

The Bachelor of Science in Cyber Security at Institution K has 100% job placement in the past two years and is the only undergraduate program in cybersecurity in Minnesota. Students learn to assess the security needs of a computer and network system, recommend safeguards and manage the implementation and maintenance of security devices, systems and procedures to protect it. These skills aim to provide students with the tools to apply what they learn to real-world problem solving.

Institution M— *Bachelor of Science in Applied Mathematics and Computer Science – Cyber Security Concentration*

Institution M's Bachelor of Science in Applied Mathematics and Computer Science with a Concentration in Cyber Security is offered on campus and prepares students for careers in software engineering, programing and networking fields. The curriculum focuses on protecting sensitive data, such as personal information, online banking and shopping safe from attacks.

Institution O — *Cyber Operations (BS)*

Institution O's Bachelor of Science in Cyber Operations is part of a 4+1 program where students have the option to complete their BS in Cyber Operations and a Master of Science in Computer Science in five years. The Cyber Operations program builds students' foundation in computing and networking with a strong understanding in network security, computer security, database design, computer programming, intranets, communications protocols, and privacy.

Institution P — *Applied Cybersecurity and Information Technology (BS)*

Illinois Tech's Bachelor of Science in Applied Cybersecurity and Information Technology focuses on cybersecurity, technology, management, compliance, and legal issues. It prepares students for careers as cybersecurity and information technology practitioners, investigators, and leaders. Students will be able to analyze and solve complex computing problems, design, implement and evaluate computer-based solutions, communicate effectively in a professional environment, and apply security principles and practices to maintain operations in the presence of risks and threats.

UPCEA

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Institution Q— *Bachelor of Science in Cybersecurity & Computer Forensics*

Institution Q's Bachelor of Science in Cybersecurity & Computer Forensics is a four-year, 120-credit program. The program covers computer and digital incident investigation, eDiscovery, network and mobile forensics, as well as legal and ethical issues in computer and computer and privacy laws. Students learn how to collect evidence against malicious acts, preserve evidence on devices, present technical evidence in court, and be familiar with security policies, electronic investigation procedures.

Institution R — *Bachelor of Science in Computer Science – Computer Networks and Security Concentration*

Institution R's Bachelor of Science in Computer Science with a Concentration in Computer Networks and Security covers a theoretical and practical understanding of the field with a focus on cybersecurity, secure programming and testing, and cyberlaw. Students are prepared to pursue careers in software engineering.

Institution S — *Bachelor of Science in Cyber and Information Security*

Institution S's Bachelor of Science in Cyber and Information Security is recognized as a Center of Academic Excellence by the National Security Agency (NSA) and the Department of Homeland Security (DHS). Students learn network security, secure software engineering, planning and budgeting in CISO Lifecyle, cloud computing and security, digital forensics, and cyber ethics, privacy and legal issues.

Institution T — *Bachelor of Science in Computer Forensics & Security*

Institution T's Bachelor of Science in Computer Forensics & Security is designed for students who are interested in technology to solve crimes or making sure computer equipment is safe and secured against hackers. The program focuses on system/network protection and forensic analysis. Students develop technical skills in computer and network security along with computer forensics.

Institution U — *Bachelor of Science in Computer Science (Engineering) – Illinois Cyber Security Scholars Program*

The Institution U's Bachelor of Science in Computer Science (Illinois Cyber Security Scholars Program) allows students to earn their degree for free and receive a stipend in exchange for working for the government for two years after they graduate.

Institution V — *Information Systems Security Bachelor's Degree*

The University of Illinois- Springfield's Bachelor of Science in Information Systems Security is designed to provide a foundation in information systems security which will include design and implementation of secure systems, security assessment and computer security ethics. Graduates will be able to demonstrate the best security practices and ethics and create secure systems that can be implemented in settings from science to the public sector or businesses.

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved

Institution W — *Cybersecurity, BS*

Institution W's Bachelor of Science in Cybersecurity covers secure coding, cryptography, digital forensics, and UNIX fundamentals with analytical thinking and criminology. Purdue uses a combination of theory and hands-on projects for students to get experience testing vulnerabilities and creating new security protocols. The University also has numerous partnerships which give students access to internships to get real-world experience.

©Copyright 2021 University Professional and Continuing Education Association, All Rights Reserved