Report*

Educator Shortage Problem Found in the 2017 CAE Cybersecurity Survey

Principal Investigator

Agnes Chan

Northeastern University

Authors

Alicia Modestino, Northeastern University

Walter McHugh, Northeastern University

Team Members

Cynthia Irvine, Naval Postgraduate School

Nancy Jones, Coastline Community College

Jake Mihevc, Mohawk Valley Community College

Tommy Morris, University of Alabama in Huntsville

*This work is supported by DoD grant no. H98230-17-1-0222. The views expressed in this material are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government. The authors would like to thank all CAE institutions for their encouragement and participation in the survey.

Table of Contents

Executive Summary

Although the government has supported programs to develop standardized cybersecurity education and training and attract more students into the field, the growth in demand for cybersecurity education has yielded a shortage of qualified cybersecurity *educators*. The current production of doctoral recipients in cybersecurity-related disciplines appears insufficient to meet demand for such educators. To determine the magnitude of the problem as well as its potential causes, we developed and administered an online survey instrument to liaisons at educational institutions belonging to the NSA/DHS Centers of Academic Excellence (CAE). The survey focused on the characteristics of current faculty, challenges in the recruitment of new cybersecurity faculty, and the impact of the faculty shortage on the number of cybersecurity courses offered.

The results from our survey indicate that a significant number of CAE institutions have difficulty filling faculty positions. This has real consequences for the nation's ability to produce cybersecurity workers. Some key findings from the report include:

- Almost half of CAE-2Y and about one-third of 4-Year CAE respondents indicated that their institution currently had a vacancy.
- Despite using a variety of recruiting channels, institutions tend to have vacancies that are open for long durations—often one to two years.
- One reason for the difficulty in recruitment is the lack of qualified applicants, with one in five CAE-2Y institutions and one in seven 4-Year CAE institutions report receiving zero qualified candidates.
- Both CAE-2Y and 4-Year CAE institutions cited losing candidates to the private sector as one of the top factors in failed searches.
- Roughly 12.0 percent of CAE-2Y and 22.2 percent of 4-Year CAE respondents indicated that between one-quarter to one-half of the courses in their catalogs had not been taught in the past three years due to a lack of cybersecurity faculty.
- Although institutions have been filling in with adjunct faculty and part-time instructors, currently there appears to be an imbalance: less than 40 percent of faculty at CAE-2Y hold a full-time tenure track position and just over 50 percent of 4-Year CAE faculty fall into this category. This limits the ability of departments to engage in curriculum design and development, provide sufficient student advising, and undertake new research.
- Although only 10-15 percent of current cybersecurity faculty are eligible to retire, that percentage is likely to rise over the next decade—exacerbating the faculty shortage and further constraining the nation's ability to build a strong cybersecurity workforce.
- Only 20 percent of doctoral recipients from 4-Year CAE institutions are seeking to enter academia upon graduation.

This report is the first part of a larger study that aims to advise the government on ways to address the cybersecurity faculty shortage. In this report, we discuss the findings of the survey including where the critical needs are, the degree of difficulty in finding qualified instructors, and the specific impediments to recruiting and retaining faculty at both 2 and 4 year institutions. In future work, we will research on ways that industry and academe can collaborate to meet the need for qualified cybersecurity instructors. At the end of the larger study, we will conclude with recommendations for programs that the government can develop with the help of the private sectors to address the shortage of cybersecurity faculty and workers.

I. Introduction

In 2013, the U.S. Department of Defense (DoD) established a cybersecurity workforce strategy in response to the growing threats posed by cybercriminals and hostile nation states (DoD 2013). This was followed by congressional legislation passed in 2014 that directed the Department of Homeland Security (DHS) to evaluate its cybersecurity capabilities and identify workforce gaps (U.S. Congress 2014). One result of these agencies' efforts was to highlight the increased demand for skilled cybersecurity personnel, both in the government sector as well as the private sector. In response, the National Institute of Standards and Technology (NIST) developed a workforce framework that provides guidance on the specific skillset that is necessary to adequately prepare U.S. cybersecurity workers to meet this demand (NIST 2016).

Yet there is growing evidence that the need for cybersecurity personnel may be outstripping the ability of U.S. educational institutions to produce such graduates. As of 2014 there were 238,158 postings for cybersecurity-related jobs nationally, accounting for 11 percent of all IT jobs (BGT 2015). Between 2010 and 2014, job postings grew by 91 percent for cybersecurity compared to only 28 percent for all IT jobs generally. In addition, cybersecurity job postings advertised salaries that were 9 percent ($6,500) higher than those for IT jobs overall and on average took 8 percent longer to fill than other IT jobs. Moreover, it appears that cybersecurity workers with particular skillsets, such as those highlighted by NIST, may be in even shorter supply. Over one-third of cybersecurity jobs call for an industry certification, compared to only one-fifth of IT jobs overall. In addition, more than 10 percent of cybersecurity job postings require a security clearance and these jobs take 10 percent on average longer to fill than cybersecurity jobs without a security clearance. Taken together, these indicators confirm that the demand for cybersecurity workers has been growing and is higher than for most other IT jobs.

The high demand for cybersecurity workers is unlikely to be met by short-term training solutions, but rather are likely to require greater capacity and coordination with higher education institutions. This is because although the skills for some IT positions can be acquired with relatively little training, cybersecurity positions typically require greater levels of both education and experience. More than 80 percent of cybersecurity job postings require at least a bachelor's

degree with at least three years of experience or five years of experience required to apply for a CISSP certification. Moreover, firms typically prefer workers with cybersecurity experience in a specific industry, like finance or health care.

Recognizing this pipeline problem, the government has developed programs to develop standardized cybersecurity training while also attracting more students into the cybersecurity field. In 1998, the National Security Agency (NSA) created the Centers of Academic Excellence (CAE) in Information Assurance Education (IAE) and Department of Homeland Security (DHS) joined in the effort as a partner in 2004. Later on, CAE-Research (CAE-R), CAE-Cyber Defense (CAE-CD) and CAE-Cyber Operations (CAE-CO) were also created to encourage institutions to offer programs in cybersecurity. In 2001, the National Science Foundation (NSF) began the CyberCorps® Scholarship for Service (SFS) program with awards to six schools to educate 198 students in the art of cybersecurity over the course of the multi-year awards.[1] By the end of 2016, the program had expanded to 62 educational institutions and supported approximately 600 students actively enrolled in cybersecurity education.[2] Recently, GenCyber, a cybersecurity program for K-12, was introduced in order to boost the pipeline for cybersecurity professionals over the longer-term.

While all these programs have been quite successful in increasing the number of *students* interested in cybersecurity, the growth in demand for cybersecurity education has yielded a shortage of qualified cybersecurity *educators*. The current production of doctoral recipients in cybersecurity-related disciplines appears insufficient to meet demand for such educators. For example, of the 1,780 doctoral degrees awarded by computer science departments at the end of the 2014-15 academic year, only 62 were awarded in the areas of information assurance and security, and of those, only 21 doctoral recipients (33.9 percent) took academic positions (Zweben and Bizot 2015). If the same trends continued, we can surmise that it would take 5 years to supply the 50 SFS institutions with two faculty members each. Furthermore, Lewis's 2017 analysis of tenure-track faculty openings across roughly 350 computer science departments revealed that the number of cybersecurity open positions remained relatively constant between

[1] National Science Foundation, NSF Scholarship for Service Awards Announced at Information Security Colloquium, https://www.nsf.gov/od/lpa/news/press/01/pr0145.htm , May 2001.
[2] Office of Personnel Management, CyberCorps®: Scholarship for Service, https://www.sfs.opm.gov , December 2016.

2016 and 2017, making it the most sought after area among all computer science disciplines (Lewis 2017). In addition, considerable anecdotal evidence indicates dozens of institutions of higher learning are seeking one or more tenure track faculty members, and many have had open job postings for several years. The shortage of a skilled cybersecurity workforce together with the lack of qualified educators, have become a real impediment to the nation's ability to build a strong cybersecurity defense.

In an effort to analyze the potential cybersecurity educator shortage, we developed and administered an online survey instrument to faculty leaders at educational institutions belonging to the NSA/DHS Centers of Academic Excellence (CAE). The survey focused on characteristics of current faculty, recruitment of new cybersecurity faculty -- including factors such as institutional support, specific areas of greatest demand, and incentives to teach—and the impact on cybersecurity degree programs and courses offered. Using this tool, we aimed to answer the following research questions:

- What are the characteristics of current cybersecurity faculty (e.g., degree, experience, field of expertise)? How many have left their positions over the past three years and why?
- What are the minimum education and experience requirements for hiring new cybersecurity faculty? Have these requirements changed over time? Are institutions able to be flexible when filling positions?
- Where are the greatest unmet needs for cybersecurity faculty? How many positions are currently open? How long do they take to fill? For which types of positions is it most difficult to recruit faculty?
- Are institutions able to attract and hire qualified candidates? How many candidates are successfully recruited? If the search was not successful, what were the primary reasons why?
- What is the current size of the degree program at their institution? What types of courses are taught? What percentage of courses have not been offered due to a lack of qualified instructors?

This report is the first part of a larger study that aims to advise NSA on ways to address the cybersecurity faculty shortage. In this report, we discuss the findings of the survey, including where the critical needs are, the degree of difficulty in finding qualified instructors, and the specific impediments to recruiting and retaining faculty at both 2- and 4-year institutions. In future work, we will conduct an industry survey to discuss ways that industry and academe can collaborate to meet the need for qualified cybersecurity instructors. At the end of the larger study, we will conclude with recommendations for programs that the government can develop with the help of the private sectors to address the shortage of cybersecurity faculty and workers.

II. Survey Methodology

This study was conducted using a survey instrument to collect quantitative data that was administered to approximately 250 CAE liaisons, including both 2 year and 4 year institutions, via email in June 2017. The survey instrument was designed to take approximately 20-30 minutes to complete, and asked detailed questions regarding the number and characteristics of current cybersecurity faculty, the number and qualifications of any open faculty positions, the types of hiring practices, the success or failure of previous faculty searches, and the number of students and courses taught at each institution.[3] The survey responses were anonymous and 120 surveys were completed by the close of the survey in August of 2017, yielding a response rate of just under 50 percent. Note that not all respondents answered every question. As a result, we report distributions for each survey question separately where the denominator is the total number of responses to that particular question, except in cases where more than one answer can be chosen (e.g. questions that ask respondents to "select all that apply").

The survey instrument was administered to CAE institutions of various designations, which are represented by both 2 and 4 year institutions, and a diversity of student body sizes, degree-granting statuses and other characteristics. Table 1 displays key characteristics of the survey respondents' institutions.

More than half of the respondents (59.5 percent) were employed in a CAE Cyber Defense (CAE-CD) institution and more than one-third were at an institution that had a CAE Research (CAE-R) designation (34.7 percent). About one quarter of the respondents came from a CAE 2

[3] See Appendix A for a full listing of the questions asked on the survey instrument.

Year (CAE-2Y) institution and less than 10 percent had a CAE Cyber Operations (CAE-CO) designation. Note that CAE member institutions can have more than one designation, except for the CAE-2Y which is mutually exclusive with the other membership types. For the remainder of the report, we refer to 4 year schools that are either CAE-CD, CAE-R, or CAE-CO members as "4-Year CAE" institutions in this report to distinguish them from CAE-2Y (i.e., 2-year) institutions.

Table 1: Key Institutional Characteristics of CAE Survey Respondents

Group	Number	%
All: Completed Responses	120	100%
CAE Designation		
CAE-2Y	32	26.4%
CAE-CD	72	59.5%
CAE-R	42	34.7%
CAE-CO	9	7.4%
(total)	121	100.0%
Institution Type		
2 Year Public	28	24.3%
2 Year Private	0	0.0%
4 Year Public	61	53.0%
4 Year Private	26	22.6%
(total)	115	100.0%
Highest Degree Conferred		
AA	25	20.8%
BA/BS	8	6.7%
MA/Prof.	24	20.0%
PhD	63	52.5%
(total)	120	100.0%
Number of Students		
< 1,000	2	2.2%
1,000 – 2,499	4	4.4%
2,500 – 9,999	14	15.6%
10,000+	70	77.8%
(total)	90	100.0%

Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Respondents could choose more than one CAE designation such that the number of responses exceeds the number of respondents.

Other institutional characteristics reported on the survey included type of institution, highest degree conferred, and number of students. Approximately one-quarter (24.3 percent) of respondents were at 2-year public institutions, another quarter were at 4-year private institutions (22.6 percent) and the remaining 53.0 percent were at 4-year public institutions. Note that some of the 2-year public institutions also indicated that they offer some 4-year degrees but are considered 2-year institutions for the purpose of NSA CAE certification and this report. Roughly half of respondents are at doctoral granting institutions (52.5 percent), with similar shares of Associate's (20.8%) and Master's/Professional (20.0%) degree institutions. Few respondents were at institutions granting only a Bachelor's degree (6.7 percent). In terms of size, about three-quarters of respondents (77.8 percent) belonged to an institution with a student body of 10,000 or more. Few respondents were located at institutions with less than 2,500 students.

III. Key Findings

In this section, we discuss the key findings from each area of the survey: characteristics of current cybersecurity faculty, recruitment of new cybersecurity faculty, and the impact on cybersecurity programs and course offerings.

A. Characteristics of Current Cybersecurity Faculty

To assess the educator pipeline problem we first take stock of the current cybersecurity faculty at CAE member institutions. Understanding the "stock," or absolute numbers and characteristics of faculty, versus the "flow" e.g. churn, loss, and recruitment of faculty in the academic market can help identify obstacles in the talent pipeline for cybersecurity educators. To measure the stock of cybersecurity faculty, the survey asked respondents for the number of current faculty at their institutions, as well as characteristics such as title, tenure status, level of degree, field of degree, and various other qualifications. In addition, the survey asked how many faculty members had left the institution and why as well as the number of retirement-eligible faculty that might be leaving in the near future.

Table 2 shows that faculty characteristics differ quite substantially by CAE designation. At CAE-2Y institutions, at least half of the faculty are part-time non-tenure track compared to 4-

Year CAE institutions where at least half of faculty are full-time tenure track. Few institutions of either type had tenure track faculty that were part-time.

Table 2: Faculty Characteristics of Institutions Responding to the Survey, by CAE Designation

	CAE-2Y		4-Year CAE	
Category	**Number**	**%**	**Number**	**%**
Full-Time, Part-Time / Tenure Status				
F/T Tenure Track	65	36.7%	456	52.7%
P/T Tenure Track	5	2.8%	18	2.1%
F/T Non-Tenure Track	18	10.2%	179	20.7%
P/T Non-Tenure Track	89	50.3%	212	24.5%
(total)	177	100.0%	865	100.0%
Faculty Title				
Adjunct	80	42.3%	258	25.5%
Instructor	38	20.1%	48	4.7%
Lecturer	10	5.3%	66	6.5%
Research Faculty	0	0.0%	28	2.8%
Teaching Faculty	10	5.3%	59	5.8%
Assistant Professor	11	5.8%	143	14.1%
Associate Professor	17	9.0%	172	17.0%
Full Professor	19	10.1%	195	19.3%
Chaired Professor	4	2.1%	43	4.2%
(total)	189	100.0%	1012	100.0%
Retirement Eligible	26	13.7%	84	8.3%

Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: "Number" refers to number of faculty in each category summed across all institutions, which is distinct from the number of respondents. Two of the 120 respondents did not indicate tenure status and four did not indicate faculty title. Due to round-off errors, the sum of the percentages may not be exactly 100%.

Table 2 also reveals that survey respondents at CAE-2Y member institutions primarily relied on adjunct faculty (42.3percent) and instructors (20.1 percent) and professors of varying ranks (27 percent). In contrast, 4-Year CAE institutions relied less on adjunct faculty (25.5 percent) and instructors (4.7 percent) and more on tenured or tenure-track faculty (54.6 percent).

Based on the survey responses, roughly 13.7 percent and 8.3 percent of the cybersecurity faculty are eligible to retire at CAE-2Y and 4-Year CAE institutions respectively.

With respect to field of study, Table 3 indicates that both CAE-2Y and 4-Year CAE institutions rely primarily on faculty with degrees in computer science (about 44 percent) and to a lesser extent, computer engineering. However, faculty at CAE-2Y institutions are more likely to specialize in information technology (23.2 percent) and compared to faculty 4-Year CAE institutions who are more likely to specialize in mathematics (13.5 percent). Across both type of institutions, cybersecurity typically ranked lower than these other fields accounting for only 7.0 percent of faculty at CAE-2Y institutions and 11.8 percent of faculty at 4-Year CAE institutions.

Table 3. Distribution of Faculty at Responding Institutions by Field of Study, by CAE Designation

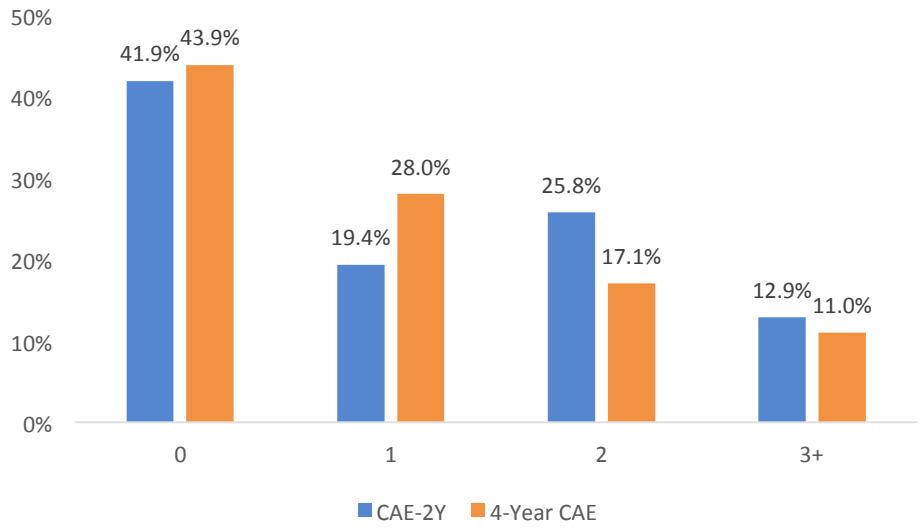
	CAE-2Y		4-Year CAE	
Degree Type / Concentration	**Number**	**%**	**Number**	**%**
Cybersecurity	13	7.0%	56	11.9%
Computer Science	82	44.3%	209	44.2%
Computer engineering	26	14.1%	52	11.0%
Information technology	43	23.2%	38	8.0%
Mathematics	5	2.7%	64	13.5%
Law	1	0.5%	12	2.5%
Criminal Justice	2	1.1%	5	1.1%
Business	6	3.2%	20	4.2%
Other	7	3.8%	17	3.6%
(Total)	185	100.0%	473	100.0%

Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: "Number" refers to number of faculty in each category summed across all institutions, which is distinct from the number of respondents. Due to round-off errors, the sum of the percentages may not be exactly 100%.

In terms of retention, respondents at both CAE-2Y and 4-Year CAE institutions indicated a loss of one cybersecurity faculty member in the last 3 years, yet there is considerable variation across institutions. Figure 1 shows that upwards of 40 percent of respondents at both CAE-2Y and 4-Year CAE institutions indicated that no faculty members had left. Among institutions that

had lost faculty, CAE-2Y institutions were most likely to lose two faculty members (25.8 percent) versus 4-Year CAE institutions that were most likely to lose just one (28.0 percent). Only 11-13 percent of either type of institution had lost more than three faculty members in the past three years.

Figure 1: Distribution of Respondents Indicating the Number of Faculty That Left Their Institution in the Past Three Years, by CAE Designation



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents = 113 with 7 respondents missing.

In addition to recording data on the number of faculty that had recently left respondents' institutions, the survey also asked respondents to indicate the primary reasons why faculty had left. Table 4 reveals that among CAE-2Y institutions, most of the time faculty left to take jobs in private industry (36.0 percent), followed by retirement (28.0 percent) and other higher education institutions (20.0 percent). While losing qualified cybersecurity faculty to the private sector further can alleviate the shortage of cybersecurity workers in the short-run, it exacerbates the long-term problem of an insufficient supply of cybersecurity workers more generally—without qualified instructors to teach, there are fewer resources to maintain or increase the supply of new cybersecurity graduates, and the shortage will persist. In contrast, 4-Year CAE institutions were more likely to lose faculty to other higher education institutions (49.3 percent), followed by

private industry (21.1 percent), and retirement (16.9 percent). While it is perhaps encouraging that fewer 4-Year CAE faculty are leaving academia, this finding gives credence to the argument that there are major pressures inside higher education to source and recruit qualified cybersecurity faculty for 4-year colleges and universities. Less than 10 percent of respondents of either CAE designation indicated that faculty were lost to the government sector, despite aggressively hiring for cybersecurity personnel and incentivizing participation in cybersecurity degree programs.

Table 4: Primary Reasons Why Faculty Left the Respondent Institution, by CAE Designation

	CAE-2Y		4-Year CAE	
Response	Number of Responses	%	Number of Responses	%
Hired by other institutions of higher education	5	20.0%	35	49.3%
Hired by private industry	9	36.0%	15	21.1%
Hired by government	1	4.0%	5	7.0%
Retirement	7	28.0%	12	16.9%
Don't know	3	12.0%	2	2.8%
Other	0	0.0%	2	2.8%
(total)	25	100%	71	100%

Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=89 with 31 missing. Respondents could choose more than one answer. Due to round-off errors, the sum of the percentages may not be exactly 100%.

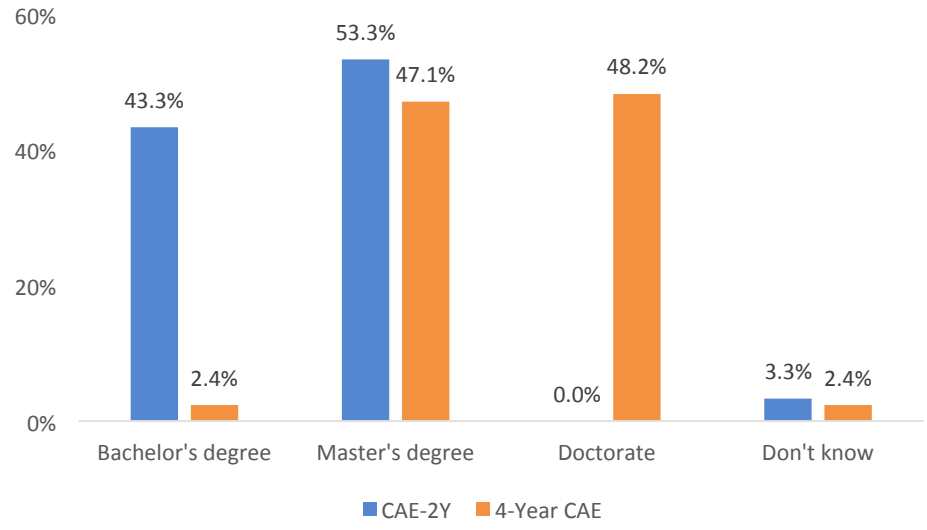
B. Required Qualifications for Hiring New Cybersecurity Faculty

What are CAE member institutions looking for in applicants, and what obstacles exist that prevent a successful faculty search? A key goal of this research is to examine CAE institutions' recruitment behaviors with respect to cybersecurity faculty and opinions on hiring outcomes to better understand the matching process between applicants and institutions. For example, stringent qualification requirements for an applicant pool of qualified, but less-credentialed, applicants could exacerbate hiring difficulties unnecessarily. It could also be the

case that applicant quality for academic positions has decreased on average if candidates with better credentials have increasingly sought higher paying positions in the private sector. To address these issues, the survey asked respondents about institutional qualifications for applicants, the quality of the applicant pool, the number of searches required to find qualified cybersecurity faculty, whether any hiring incentives were offered, and, critically, what factors may have contributed to failed faculty searches at their institutions (if any).

We began our inquiry into the recruitment of new cybersecurity faculty by asking respondents to list the minimum required qualifications for education and experience. Not surprisingly, Figure 2 reveals that minimum degree requirements were higher among 4-Year CAE versus CAE-2Y institutions. Just over half of CAE-2Y institutions required a Master's degree (53.3 percent) with most of the remaining institutions requiring only a Bachelor's degree (43.3 percent) and none requiring a Ph.D. In contrast, just under half of 4-Year CAE institutions required a Ph.D. (48.2 percent) with most of the remaining institutions requiring only a Master's degree (53.3 percent).

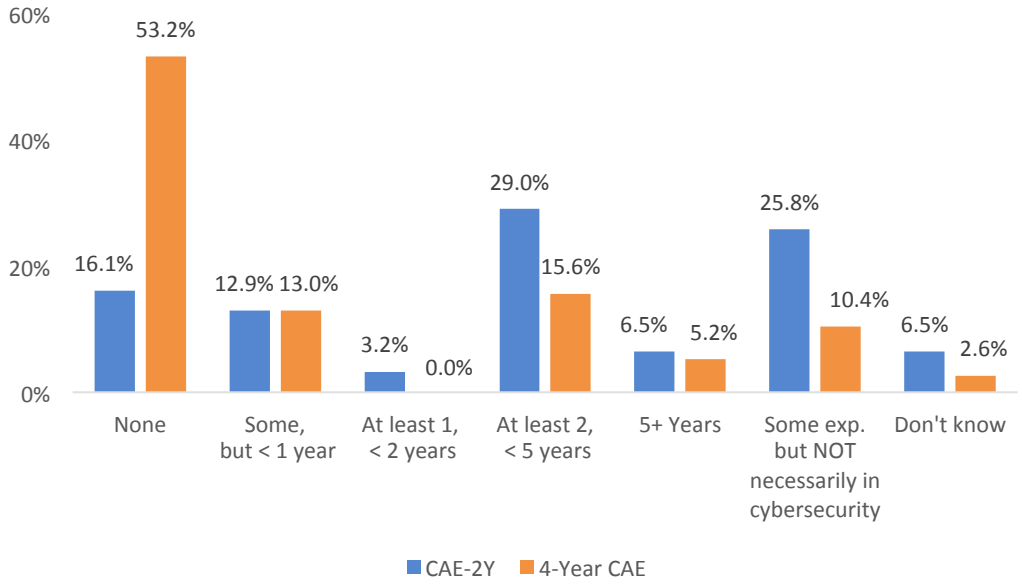
Figure 2: Distribution of Minimum Degree Requirements at Responding Institutions, by CAE Designation



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=115 with 2 missing and 3 indicating "Not Applicable".

In terms of work experience, the reverse was true with CAE-2Y institutions requiring more experience than 4-Year CAE institutions. Roughly 84 percent of CAE-2Y institutions require some experience, most frequently in the range of 2-5 years (29.0 percent) and not necessarily in cybersecurity (25.8 percent). In contrast, less than half of 4-Year CAE institutions required any experience (46.8 percent), with 13.0 percent requiring less than one year and 15.6 percent requiring 2-5 years. This is consistent with anecdotal observations that 4-Year CAE institutions place a greater emphasis on faculty that engage in academic research whereas CAE-2Y institutions place more weight on practitioners who often continue to work in applied settings. Looking at the cross-tabulations reveals that, in general, the greater the education requirement, the lower the years of experience required.

Figure 3: Distribution of the Minimum Work Experience Requirements at Responding Institutions, by CAE Designation

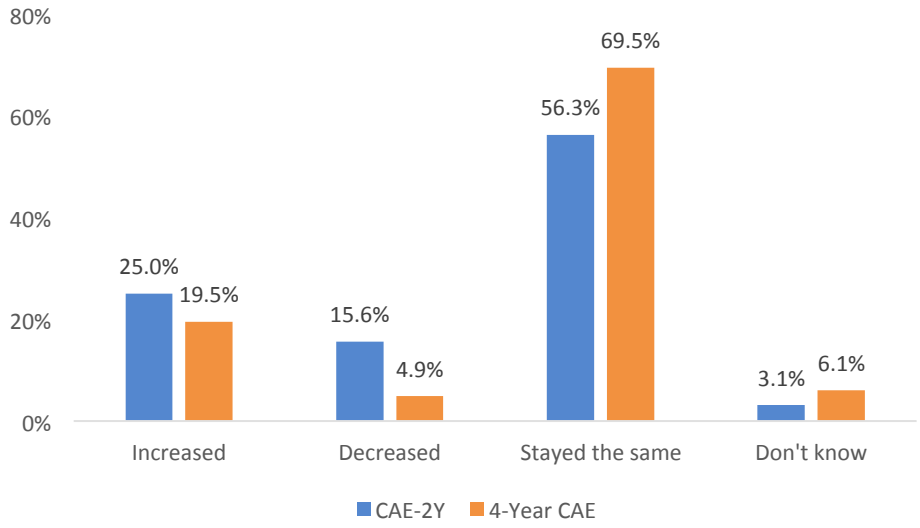


Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=108 with 2 missing and 10 indicating "Not Applicable".

We also investigated whether the minimum education and experience requirements for cybersecurity faculty applicants had changed over time. This is important because increasing skill requirements could limit the pool of qualified applicants and possibly increase the probability of a failed search. On the other hand, decreasing skill requirements may indicate that

institutions are responding to the lack of qualified candidates in the labor market. Figure 4 shows that minimum degree qualifications were more likely to have stayed the same at 4-Year CAE (69.5 percent) versus CAE-2Y (56.3 percent) institutions. Yet across both institutional types, if qualifications had changed, they were more likely to increase than to decrease. This "upskilling" trend was somewhat stronger among the CAE-2Y institutions with of 25.0 percent of respondents indicating that degree requirements had increased compared to only 19.5 percent of 4-Year CAE institutions. However, CAE-2Y institutions were also more likely to indicate that they had decreased degree requirements compared to 4-Year CAE institutions (15.6 percent versus 4.9 percent). This suggests that, in terms of degree requirements, the labor market for CAE-2Y educators is more fluid than that for 4-Year CAE faculty and skill requirements are more responsive to market conditions-likely because there is a greater supply of individuals with Bachelor's and Master's degrees related to cybersecurity.

Figure 4: Distribution of Changes in Minimum Degree Qualifications over the Past 5 Years, by CAE Designation

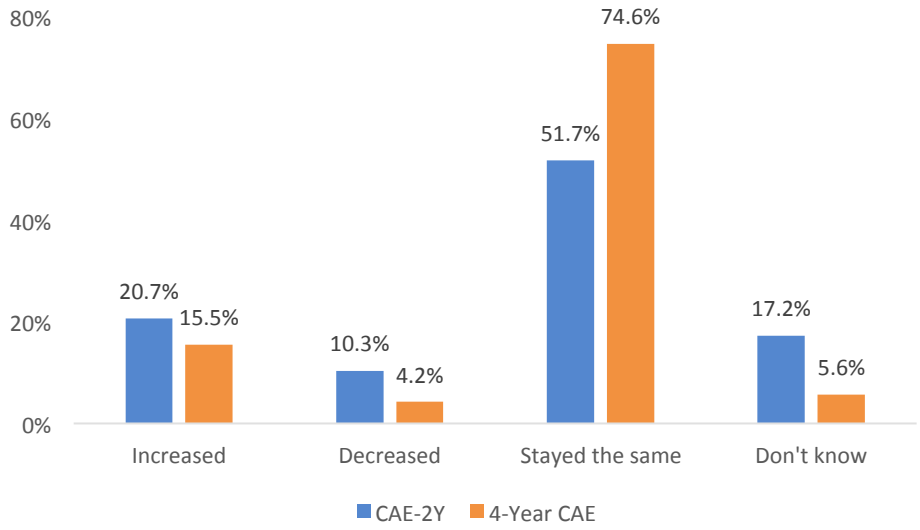


Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=114 with 6 missing and 4 responding "Not Applicable".

We found a very similar pattern of changes in work experience as well, although the difference between CAE-2Y and 4-Year CAE institutions is even starker. While roughly half of CAE-2Y respondents say that experience requirements have stayed the same, about three-

quarters of 4-Year CAE respondents report no change (see Figure 5). This could reflect that CAE-2Y institutions often place a greater emphasis on experience and as such, may need to adjust their requirements more frequently as labor market conditions change. Indeed, there was a high degree of uncertainty among CAE-2Y institutions with 17.2 percent indicating they did not know whether the experience qualifications at their institution had changed compared to only 5.6 percent of respondents at 4-year CAE institutions who were uncertain about changes in requirements.

Figure 5: Distribution of Changes in Minimum Work Experience Qualifications over the Past 5 Years, by CAE Designation

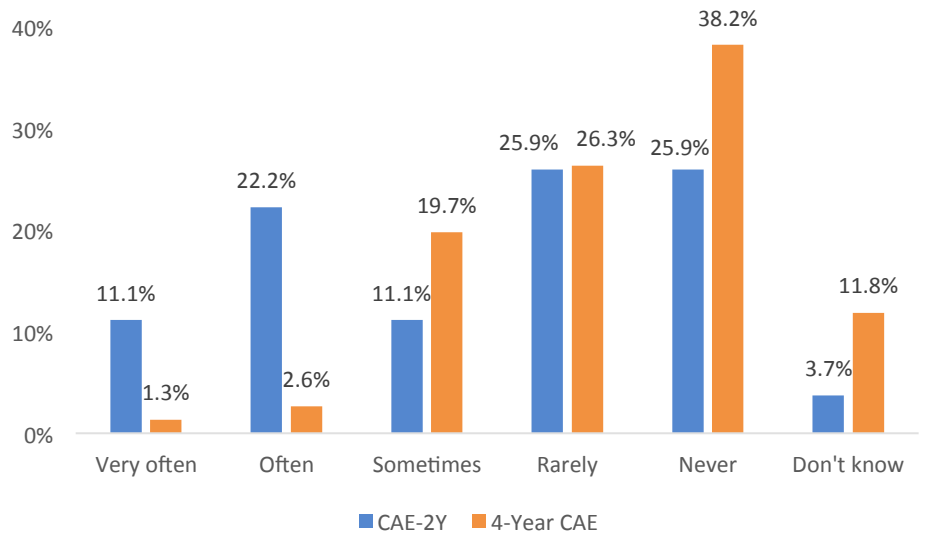


Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=100 with 3 missing and 17 "Not Applicable".

To better gauge whether the minimum requirements listed above were binding when recruiting faculty, we also asked respondents whether their institutions had made exceptions. If yes, then this would suggest a greater degree of flexibility in hiring than what is stated in a job posting. It would also indicate the degree to which the number of cybersecurity faculty might be expanded by lowering some of the posted requirements to attract more candidates. Based on the responses to the survey, it appears that while CAE-2Y institutions were willing to make

exceptions to the minimum qualifications they advertised for their positions, while 4-Year CAE institutions were not. Figure 6 shows that among CAE-2Y institutions, roughly one in three respondents indicated that they "often" or "very often" made exceptions to the typical minimum qualifications whereas only 3.9 percent of 4-Year CAE respondents indicated such a willingness to be flexible when making hiring decisions. In fact, the majority of respondents from 4-Year CAE institutions (64.5 percent) indicated that their institution "rarely" or "never" makes such exceptions. The comparative rigidity of 4-year institutions may reflect the priority that the institutions themselves or the accrediting bodies place on the credentials of the personnel they hire. The flexibility observed among CAE-2Y institutions may suggest an alternative path to filling positions that are in high demand is needed, as long as the overall quality of instruction does not decrease.

Figure 6: Frequency of Exceptions Made to Typical Minimum Qualifications to Recruit Cybersecurity Faculty, by CAE Designation



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=103 with 2 missing and 15 responding "Not Applicable".

In addition to formal education and experience requirements, institutions often seek individuals with a particular field of specialization, to either complement or substitute the expertise of existing faculty. Having preferences beyond the requirements stated in a job posting may also decrease the likelihood of filling a vacant position, even if there are qualified

candidates in terms of education and experience. We explored this in depth for the CAE-2Y institutions by asking detailed questions about specific requirements that are often not listed in a job posting. For example, Table 5 shows the distribution of specializations that CAE-2Y institutions were most interested in hiring at various levels (introductory, intermediate, and advanced). Across all levels, institutions were most interested in fundamentals of security followed by networking and then systems. Risk analysis and auditing were also sought after at the introductory level. Other preferences among CAE-2Y were fairly minimal. For example, of the institutions that specified a minimum teaching experience the levels that was preferred was part-time experience at the community college level. Only 15 percent of CAE-2Y institutions required that their faculty be able to teach all courses in the discipline for which they were hired. However, other types of experience were highly valued, with about 40 percent of CAE-2Y institutions requiring candidates have formal curriculum development experience, and over 80 percent preferring candidates had experience with K-12 outreach or cyber competitions. [4]

Table 5: Distribution of Field of Specialization that Institutions were Most Interested in Hiring, CAE-2Y Only

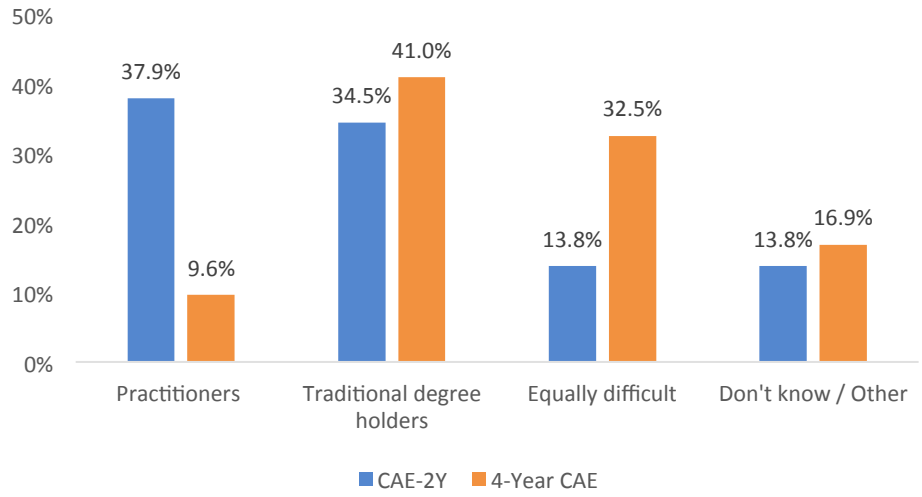
Specialization	Introductory (Column %)	Intermediate (Column %)	Advanced (Column %)
Fundamentals of Security	28.1%	24.5%	32.0%
Networking	20.3%	34.7%	32.0%
Systems	15.6%	24.5%	12.0%
Business Management	6.3%	4.1%	4.0%
Risk analysis/Auditing	15.6%	6.1%	4.0%
Legal/Policy	10.9%	2.0%	4.0%
Other	1.6%	2.0%	8.0%
Don't know	0.0%	0.0%	0.0%
“Not Applicable”	1.6%	2.0%	4.0%
(Total)	100.0%	100.0%	100.0%
(Total Count)	64	49	25

Source: Authors’ calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Due to round-off errors, the sum of the percentages may not be exactly 100%.

[4] See Appendix B for these additional results pertaining only to CAE-2Y institutions.

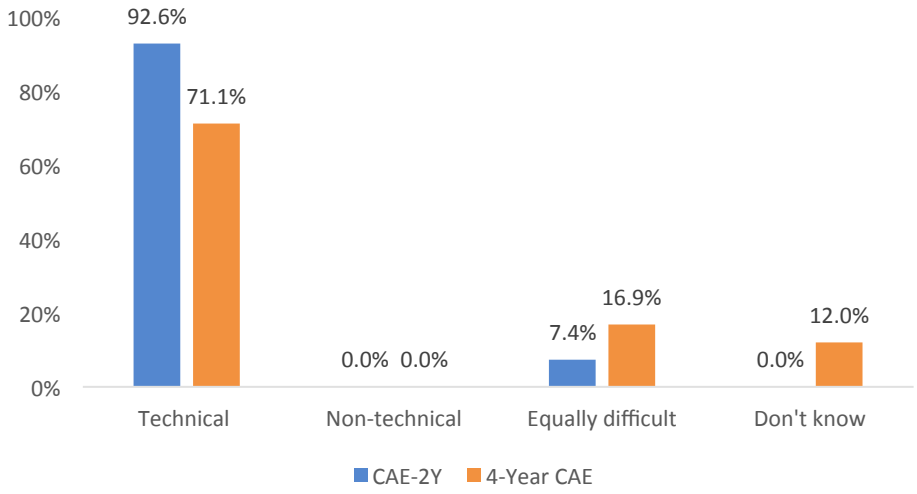
Finally, we asked respondents which qualifications made it more difficult to recruit candidates for cybersecurity faculty positions. Figure 7 shows that while both types of institutions found it difficult to recruit traditional degree holders, CAE-2Y institutions were more likely to report that it was difficult to recruit practitioners (37.9 percent) compared to 4-Year CAE institutions (9.6 percent). Figure 8 confirms that the majority of institutions find it most difficult to recruit technical versus non-technical faculty, although the share is much higher among CAE-2Y institutions (92.6 percent) versus 4-Year CAE institutions (71.1 percent).

Figure 7: Difficulty in Recruiting Practitioners versus Traditional Degree Holders, by CAE Designation



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=112 with 2 missing and 6 responding "Not Applicable".

Figure 8: Difficulty in Recruiting Technical versus Non-Technical Faculty, by CAE Designation

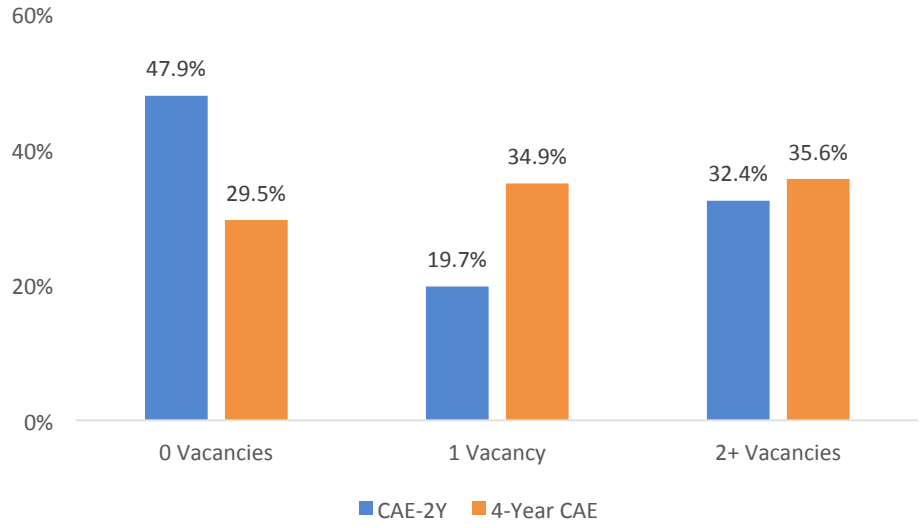


Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=110 with 4 missing and 6 responding "Not Applicable".

C. Recruitment Practices for Hiring Cybersecurity Faculty

One of the key issues that we sought to quantify was the intensity of demand for cybersecurity faculty at CAE institutions. We measured this in several ways including the number of vacancies, the duration of open positions, the variety of recruiting channels, and the number of failed searches. Figure 9 (below) displays the shares of respondents indicating the number of open positions (new or vacant) for cybersecurity faculty that their institution had at the time of the survey, and the expected number of such openings over the next year. Almost half of CAE-2Y respondents indicated that their institution had zero vacancies—in contrast, less than one-third of 4-Year CAE respondents reported no job openings. Much of the difference between the two types of institutions was due to a higher share of 4-Year CAE institutions with just one vacancy (32.9 percent compared to only 19.7 percent for CAE-2Y). Similar shares of both types of institutions (about one-third) had two or more vacancies to fill.

Figure 9: Percent of Respondents Indicating the Number of Vacancies for Cybersecurity Faculty Positions at their Institution Currently or Over the Next Year, by CAE Designation



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=95 with 4 missing, 5 responding "Not Applicable" and 16 "Don't know."

We can also estimate the overall distribution of the type of vacancies among CAE institutions. Specifically, we multiply the number of responses for each vacancy count (e.g., 0, 1, 2, …) by the number of respondents in each category (e.g., FT tenure-track, PT tenure track, …) to get the total number of vacancies for that category. We then calculate the percentage of vacancies in each category as a share of the total number of vacancies across all categories. Table 6 shows that across all CAE-2Y institutions that responded to the question, over 40 percent of vacant positions were for adjunct faculty while another quarter were for full-time tenure track faulty. The reverse was true across all 4-Year CAE institutions that responded to the question, where over 40 percent of vacant positions were for full-time tenure track faculty and about one-quarter were for adjunct faculty. Across both institutional types, part-time non-tenure track faculty were the next most frequent opening.

Table 6: Distribution of Vacancies by Type of Position, by CAE Designation

Type of Position	CAE-2Y Count	CAE-2Y %	4-Year CAE Count	4-Year CAE %
Full-Time, Part-Time / Tenure Status				
F/T tenure-track	20	26.7%	88	42.9%
P/T tenure-track	0	0.0%	1	0.5%
F/T non-tenure track	9	12.0%	16	7.8%
P/T non-tenure track	14	18.7%	23	11.2%
Research faculty	0	0.0%	10	4.9%
Teaching faculty	1	1.3%	10	4.9%
Instructor	0	0.0%	7	3.4%
Adjunct	31	41.3%	50	24.4%
(total)	75	100.0%	205	100.0%

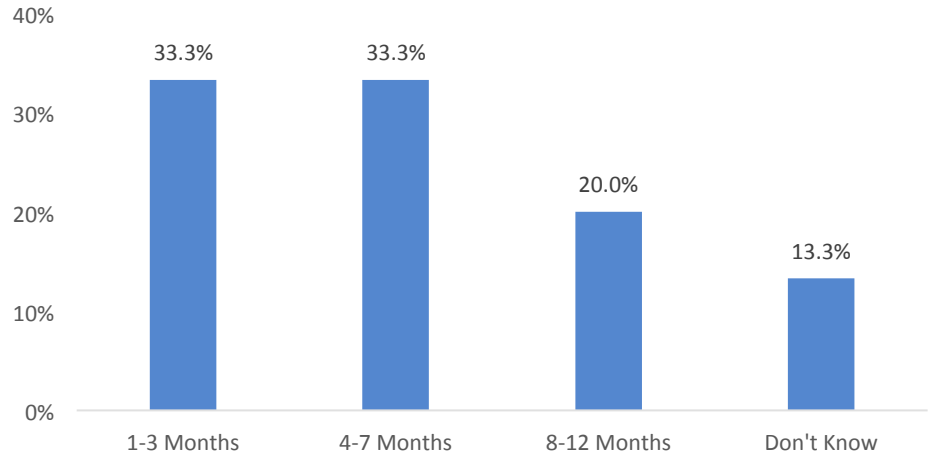
Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=95 with 4 missing, and 5 responding "Not Applicable" and 16 "Don't know.". Due to round-off errors, the sum of the percentages may not be exactly 100%.

To more accurately measure the difficulty in recruiting, the survey also asked respondents how many months any of the vacant cybersecurity positions at their institution had been open. This is important because having a high number of vacancies may simply indicate a high level of churn in the labor market if positions are filled quickly. However, if it is the case that vacancies stay open for long periods, then this is usually an indication that there is either a shortage of workers or some other barrier to recruitment. The average vacancy duration for all jobs in the economy is roughly one month—jobs that take more than three months to fill are typically considered a long-term vacancy. That said, it is likely that job openings in academia have longer durations due to the need to plan in advance for the upcoming academic year.

Figures 10 and 11 show the distribution of vacancies by selected durations for CAE-2Y and 4-Year CAE institutions respectively. Comparing the two distributions shows that 4-Year CAE institutions tend to have vacancies that are open longer than CAE-2Y institutions. Whereas

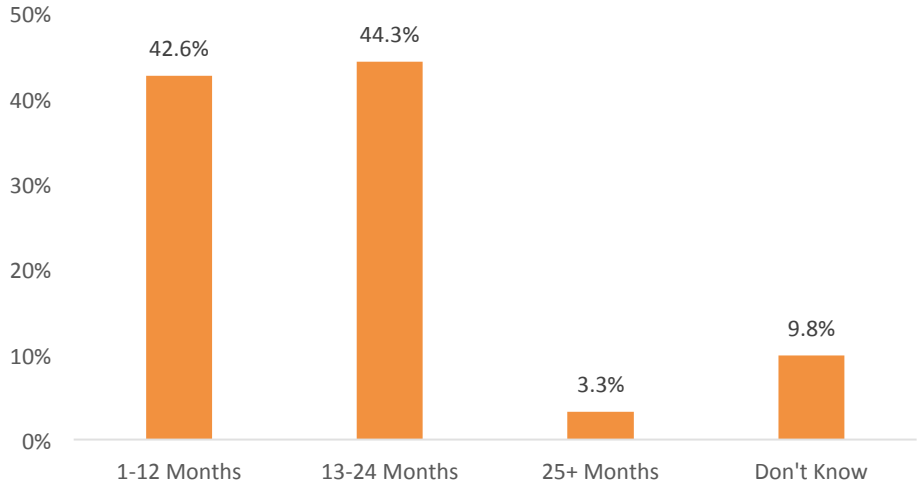
most cybersecurity faculty positions at CAE-2Y institutions are filled within 7 months and 87 percent are filled within a year, only 42.6 percent of cybersecurity faculty positions at 4-Year CAE institutions were filled so quickly. Another 44.3 percent of cybersecurity faculty vacancies at 4-Year CAE institutions took between one to two years to fill and another 3.3 percent took more than two years. It is unlikely that durations of this magnitude among 4-Year CAE institutions simply reflect planning for the upcoming academic year, but rather reflect the difficulty that 4-Year CAE institutions have in filling cybersecurity positions. However, one should interpret this finding with caution as fewer than half of the 4-Year CAE respondents answered this question.

Figure 10: Distribution of Durations for Cybersecurity Faculty Vacancies, CAE-2Y Institutions



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=13 with 9 missing and 10 responding "Not Applicable".

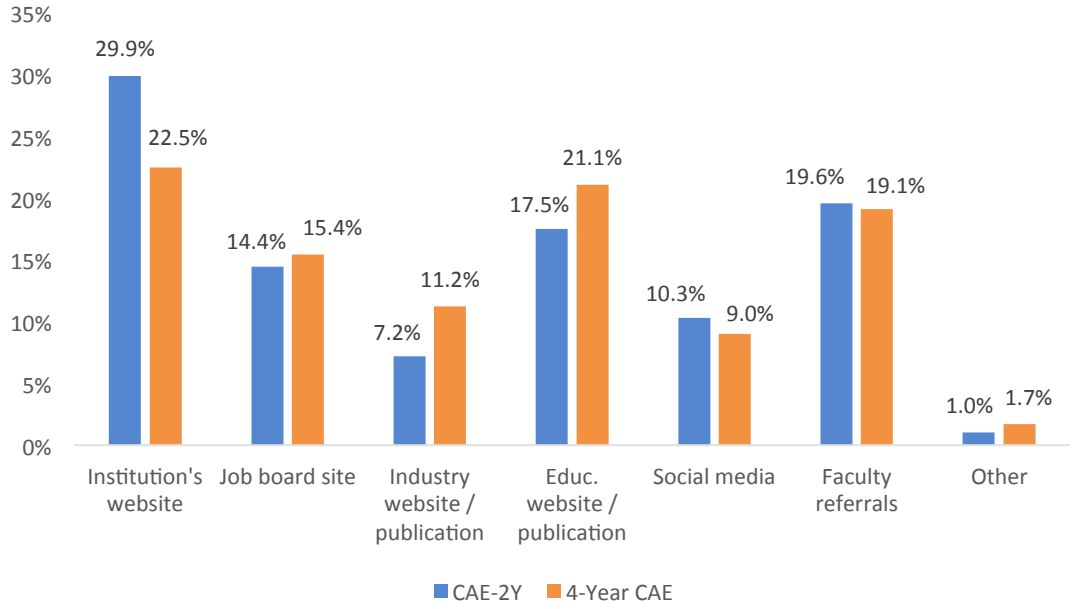
Figure 11: Distribution of Durations for Cybersecurity Faculty Vacancies, 4-Year CAE Institutions



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=39 with 23 missing and 26 responding "Not Applicable".

The amount of resources required to source, vet, and hire for cybersecurity faculty indicates the recruitment intensity undertaken by the institution—another indicator of whether these positions are particularly difficult to fill. For example, posting a vacancy in places other than the institution's web site, such as a job board or industry publication, which likely charge a fee, would indicate that the institution is searching more intensively for applicants. Figure 12 displays the recruitment channels used by institutions when advertising open cybersecurity faculty positions. CAE-2Y institutions are more likely to rely on their own web sites for advertising positions (29.9 percent) compared to 4-Year CAE institutions (22.5 percent) which more frequently use job board sites, industry websites or publications, and education websites or publications. This difference might also reflect that recruiting at CAE-2Y institutions tend to be more localized compared to 4-Year CAE institutions that often conduct nationwide or even global searches. About 10 percent of both types of institutions use social media and about 20 percent rely on faculty referrals.

Figure 12: Distribution of Recruitment Channels Used to Advertise Open Cybersecurity Positions, by CAE Designation



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=116 with 2 missing and 2 responding "Not Applicable".

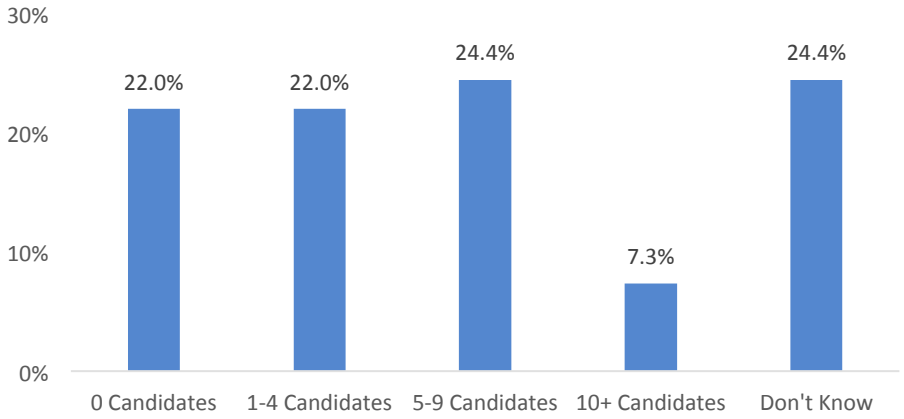
D. Applicant Pool for Cybersecurity Faculty Searches

One potential impediment to hiring cybersecurity faculty is an applicant pool simply lacking in sufficient education or skill. The survey instrument includes questions to examine both "stocks" of applicants, i.e. how many *qualified* applicants typically apply to cybersecurity jobs, and also perceptions about how the qualifications of applicants have been changing over time. Specifically, we asked respondents to estimate the number of qualified candidates that typically apply to their institution's cybersecurity faculty positions for various types of faculty roles. Figures 12 and 13 report the distributions for CAE-2Y and 4-Year CAE institutions respectively.

In general, 4-Year CAE institutions receive a higher number of qualified candidates than CAE-2Y institutions, although there is a high degree of uncertainty among respondents at both institutions. This is likely because faculty typically do not know such information unless they recently have served on the hiring committee. Nevertheless, 22.0 percent of CAE-2Y institutions and 14.5 percent of 4-Year CAE institutions report receiving *zero* qualified candidates. About

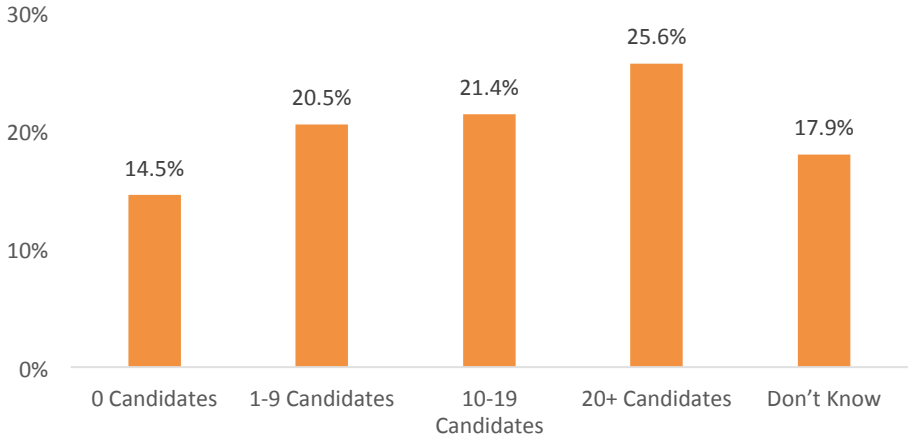
46.4 percent of CAE-2Y institutions receive 1-9 qualified applicants compared to only 20.5 percent of 4-Year CAE institutions. In contrast, 47 percent of 4-Year CAE institutions report receiving 10 or more candidates compared to only 7.3 percent of CAE-2Y institutions. The greater lack of qualified candidates at CAE-2Y institutions may reflect both quantity (e.g., a smaller applicant pool if most hiring is done locally) as well as quality (e.g. fewer applicants with cybersecurity experience versus programming experience).

Figure 13: Distribution of Qualified Cybersecurity Applicants Applying to Positions, CAE-2Y Institutions



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=26 with 1 missing and 5 responding "Not Applicable".

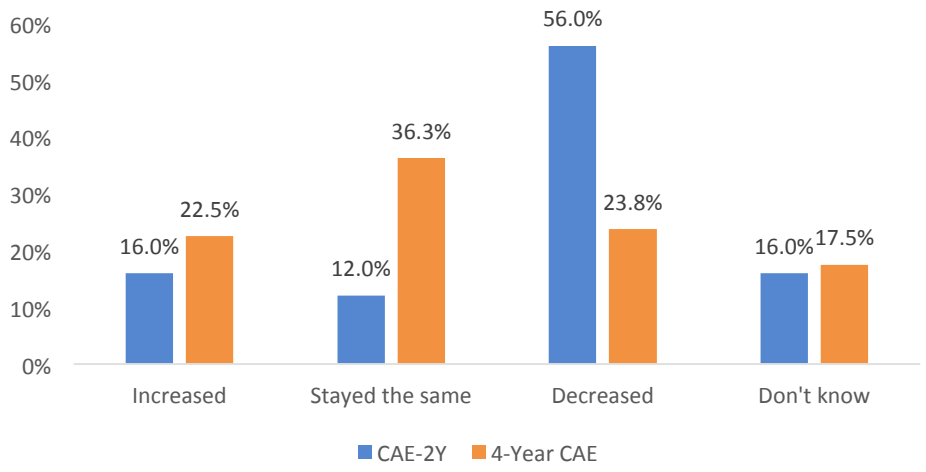
Figure 14: Distribution of Qualified Cybersecurity Applicants Applying to Positions 4-Year CAE Institutions



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=73 with 8 missing and 7 responding "Not Applicable".

We also sought to determine whether the number of applicants had changed over the past three years to determine whether the market for cybersecurity educators was becoming tighter. Figure 15 indicates that although 36.3 percent of 4-Year CAE institutions detected no change in the number of qualified applicants, this was the case for only 12.0 percent of the CAE-2Y institutions. This is because nearly 60 percent of CAE-2Y institutions responded that the number of qualified candidates had decreased—as was apparent in the lower number of applicants they receive compared to the 4-Year CAE institutions. The decrease in qualified candidates among CAE-2Y institutions over time may reflect increasing competition with private sector employers as the labor market continued to strengthen after the Great Recession (Rich, 2013). Only 16.0 percent of CAE-2Y and 22.5 percent of 4-Year CAE institutions indicated that the number of qualified applicants for cybersecurity faculty positions had increased.

Figure 15: Change in the Number of Qualified Applicants for Cybersecurity Positions over the Past Three Years, by CAE Designation



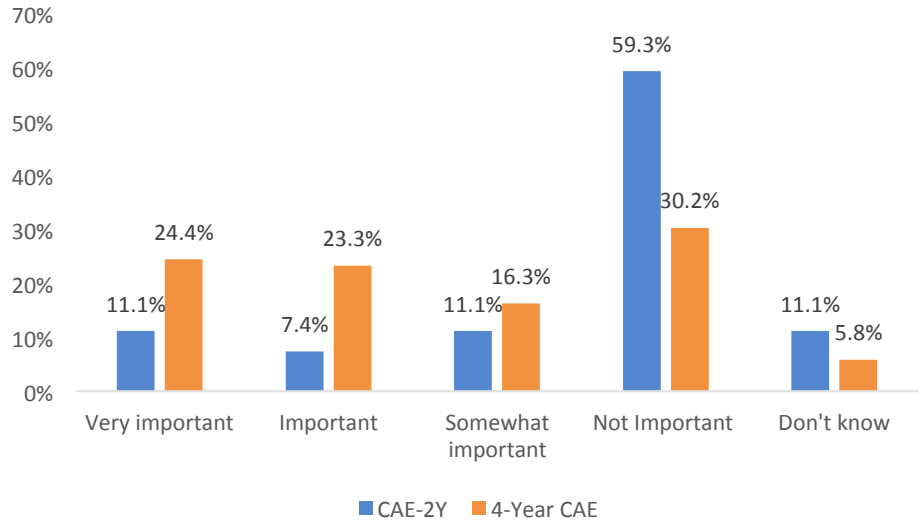
Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey
Note: Number of respondents=105 with 5 missing and 10 responding "Not Applicable".

Many employers that recruit workers in STEM field often make use of the H1-B visa program which allows U.S. employers to employ foreign workers in "specialty occupations" that require "theoretical and practical application of a body of highly specialized knowledge" as well as a bachelor's degree. The program sets a cap each year on the number of H1-B visas that will be issued and is typically oversubscribed with employers often reaching the cap in the first few

months of each year. For example, of the 348,669 H1-B visa applicants in 2015, only 275,317 were approved with roughly 20 percent of applications denied. Under the Trump administration the cap is likely to be lower with the U.S. Citizenship and Immigration Service temporarily suspending premium processing for all H-1B visa petitions in April 2017 as part of President Trump's "*Buy American, Hire American*" Executive Order which directed federal agencies to propose reforms to the H-1B visa system.

Since cybersecurity falls under the set of occupations that would be eligible for the H1-B visa program, we examined whether foreign born workers were an important source of faculty for the CAE institutions. Figure 16 indicates that a higher share of 4-Year CAE institutions responded that non-citizens were either "very important" or "important" as a recruiting source (47.7 percent) compared to only 18.5 percent of CAE-2Y institutions. In fact nearly 60 percent of CAE-2Y institutions responded that foreign-born workers were "not important" as a potential source of faculty. The lack of foreign candidates at CAE-2Y institutions may reflect fewer resources to engage in the complexities of the H1-B visa program as well as a greater emphasis on the need for faculty with recent cyber workforce experience in the U.S.

Figure 16: Importance of Non-Citizens / Non-Permanent Residents as a Source of Cybersecurity Faculty, by CAE Designation



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=113 with 2 missing and 5 responding "Not Applicable".

Indeed, both CAE-2Y and 4-Year CAE institutions indicate that individuals from industry who teach during non-work hours are their primary source of adjunct faculty. Table 7 indicates that 66.7 percent of CAE-2Y and 85.7 percent of 4-Year CAE institutions rely on such candidates as their primary source of hiring for adjunct faculty. Individuals from government or those who teach at multiple institutions most often ranked second as a source for adjunct faculty. Semi-retired individuals and graduate students from other universities were more likely to be ranked third. These findings suggest that losing candidates to the private sector may not be a total loss if those individuals eventually teach part-time as adjuncts. It also suggests that there may be an opportunity for institutions to build partnerships with industry to facilitate employees teaching part-time during non-work hours.

Table 7: Top Three Primary Sources for Hiring Adjunct Cybersecurity Faculty, by CAE Designation

Response	Rank 1 %	Rank 2 %	Rank 3 %	Total %	Total Count
CAE-2Y Institutions					
Individuals from industry who teach during non-work hours	66.7%	26.7%	6.7%	100.0%	30
Individuals from government labs or other government organizations who teach during non-work hours	28.6%	42.9%	28.6%	100.0%	14
Individuals who teach at multiple institutions as an adjunct	6.7%	53.3%	40.0%	100.0%	15
Semi-retired individuals	13.3%	40.0%	46.7%	100.0%	15
Graduate students from other institutions	0.0%	0.0%	100.0%	100.0%	1
4-Year CAE Institutions					
Individuals from industry who teach during non-work hours	85.7%	8.2%	6.1%	100.0%	49
Individuals from government labs or other government organizations who teach during non-work hours	17.1%	65.7%	17.1%	100.0%	35
Individuals who teach at multiple institutions as an adjunct	20.0%	50.0%	30.0%	100.0%	20
Semi-retired individuals	21.1%	42.1%	36.8%	100.0%	19
Graduate students from other institutions	20.0%	20.0%	60.0%	100.0%	5

Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Respondents may choose multiple options. Due to round-off errors, the sum of the percentages may not be exactly 100%.

The primary reasons why adjunct cybersecurity faculty choose to teach are very similar across institution types. Table 8 shows that the most highly ranked reasons include to earn extra compensation and also because adjunct faculty enjoy teaching. Among secondary reasons, adjuncts were more likely to teach at CAE-2Y institutions out of a send of civic duty compared to 4-Year CAE institutions where they were more likely to teach as a way to transition to a career in academia. Earning continuing education credits and recruiting future colleagues ranked a distant third. These findings would suggest that institutions may want to consider raising compensation for adjuncts or establishing more "teaching faculty" positions that are part-time as a way to increase the capacity of their cybersecurity departments.

Table 8: Top Three Reasons Why Adjunct Cybersecurity Instructors Choose to Teach, by CAE Designation

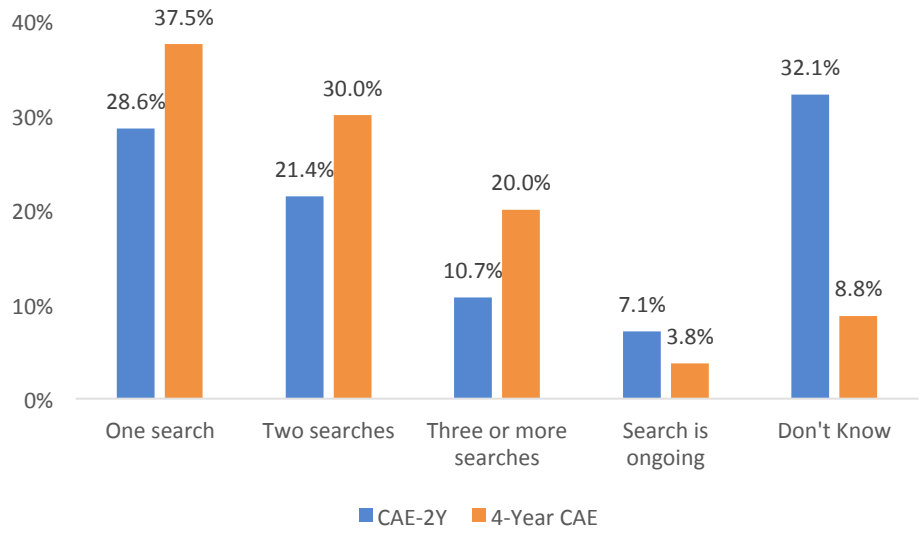
Response	Rank 1 %	Rank 2 %	Rank 3 %	Total %	Total (Count)
CAE-2Y Institutions					
To earn extra compensation	61.9%	19.0%	19.0%	100.0%	21
Because they enjoy teaching	50.0%	38.9%	11.1%	100.0%	18
Because of a sense of civic duty or patriotism	23.1%	53.8%	23.1%	100.0%	13
As a way to transition to a career in academia	14.3%	28.6%	57.1%	100.0%	14
To earn Continuing Education Credits (CEU's) to maintain certifications	16.7%	33.3%	50.0%	100.0%	6
To recruit future colleagues	0.0%	100.0%	0.0%	100.0%	2
4-Year CAE Institutions					
To earn extra compensation	62.5%	27.5%	10.0%	100.0%	40
Because they enjoy teaching	50.0%	30.6%	19.4%	100.0%	36
Because of a sense of civic duty or patriotism	44.4%	27.8%	27.8%	100.0%	18
As a way to transition to a career in academia	20.0%	33.3%	46.7%	100.0%	30
To earn Continuing Education Credits (CEU's) to maintain certifications	20.0%	40.0%	40.0%	100.0%	5
To recruit future colleagues	33.3%	50.0%	16.7%	100.0%	6

Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Respondents may choose multiple options. Due to round-off errors, the sum of the percentages may not be exactly 100%.

E. Effectiveness of Recent Cybersecurity Faculty Searches

Finally, we also directly examined respondents' perceptions of the effectiveness of faculty search as well as the reasons why they thought a search had failed and whether any special incentives had been used to entice applicants to accept a position. Figure 17 shows the distribution of the number of searches required to fill a cybersecurity vacancy for both CAE-2Y and 4-Year CAE institutions. Surprisingly, upwards of one-third of CAE-2Y respondents did not know how many searches were needed compared to less than 10 percent of 4-Year CAE institutions. Perhaps this is because the search process is more centralized at CAE-2Y institutions and involves fewer faculty compared to 4-Year CAE institutions. This lack of knowledge makes it difficult to compare the responses across institutions. Nevertheless, it appears that the most common outcome for both institutions is to fill a position based on one search—although that percentage is still not a majority of institutions. For example, among 4-Year CAE institutions, only 37.5 percent of respondents indicated that they were able to fill a cybersecurity position after just one search. Another 30.0 percent required two searches and 20.0 percent required three or more searches.

Figure 17: Distribution of Number of Searches Required to Fill a Cybersecurity Vacancy, by CAE Designation



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=108 with 6 missing and 6 responding "Not Applicable".

One of the most singularly important aspects of this research is to determine why such a high fraction of cybersecurity faculty searches are failing. While we could not directly ask applicants who declined positions at CAE institutions why they did so, we did collect data on respondents' opinions on why their institution's cybersecurity faculty search had failed. Respondents were asked to rank their top three "primary reasons" they attributed to their department's lack of success in recruiting candidates which included a range of professional reasons associated with the institution as well as personal factors related to the candidate.

Table 9 demonstrates that the reasons why searches fail differ somewhat by the type of institution. Losing candidates to the private sector ranked among the top two factors cited for both types of institutions (roughly 20 percent). However, while non-competitive salaries ranked highly for CAE-2Y institutions, losing candidates to other academic institutions was a top reason for failed searches for 4-Year CAE institutions. Secondary considerations included losing candidates to the government sector for CAE-2Y institutions (13.3 percent) and difficulties with dual career location choices for 4-Year CAE institutions (16.1 percent). Both types of institutions reported choosing not to make an offer because the candidate was unqualified as a top reason about 10 percent of the time. Other reasons that do not seem to be primary factors driving failed searches had fewer than 5 percent of responses including the balance of teaching and research, the number of "advanced" students, and the class sizes at the institution as well as competing post-doc opportunities for new Ph.Ds.

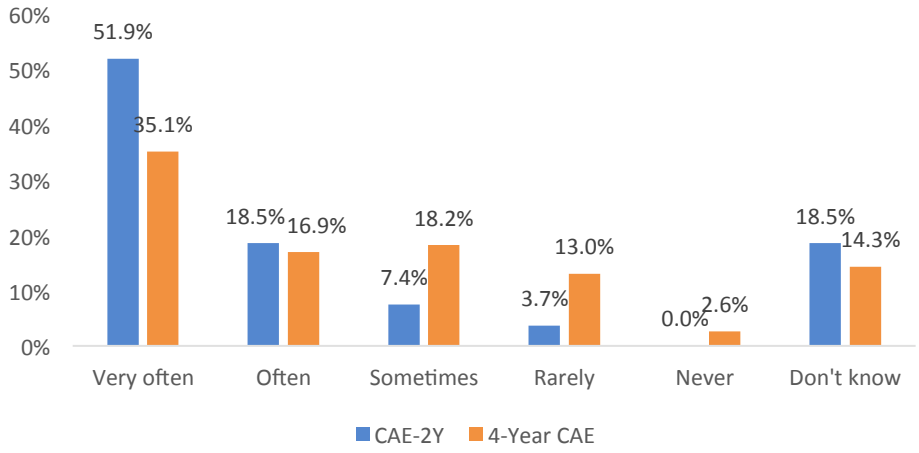
Table 9: Top Reasons Why Cybersecurity Faculty Searches Were Unsuccessful by CAE Designation

Response	CAE-2Y	4-Year CAE
Our department chose not to make an offer because candidate was not qualified	13.3%	10.8%
Candidate cited the salaries at our institution were too low/not competitive	20.0%	9.7%
Candidate chose position in private sector	23.3%	18.3%
Candidate chose position in government sector	13.3%	1.1%
Candidate chose position in another academic institution	13.3%	32.3%
Candidate chose to stay at current institution	3.3%	5.4%
Candidate chose position near their spouse/significant other	6.7%	16.1%
TOTAL	93.3%	93.5%

Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=116 with 4 missing.

To probe more deeply into whether low salaries are a common reason why searches may be failing, we also asked respondents to indicate the frequency with which candidates cite that salary is too low when they reject offers, a subtle but important difference. For example, although salary was not one of the most prevalent factors for failed searches among 4-Year CAE institutions, it may still be a contributing factor that makes employment in the private sector or another institution more attractive. Indeed, Figure 18 shows that over half of 4-Year CAE institutions and more than 70 percent of CAE-2Y reported that salary was "very often" or "often" cited by candidates as too low or not competitive.

Figure 18: Frequency of Applicants Citing Salary Offer is Not Competitive, by CAE Designation

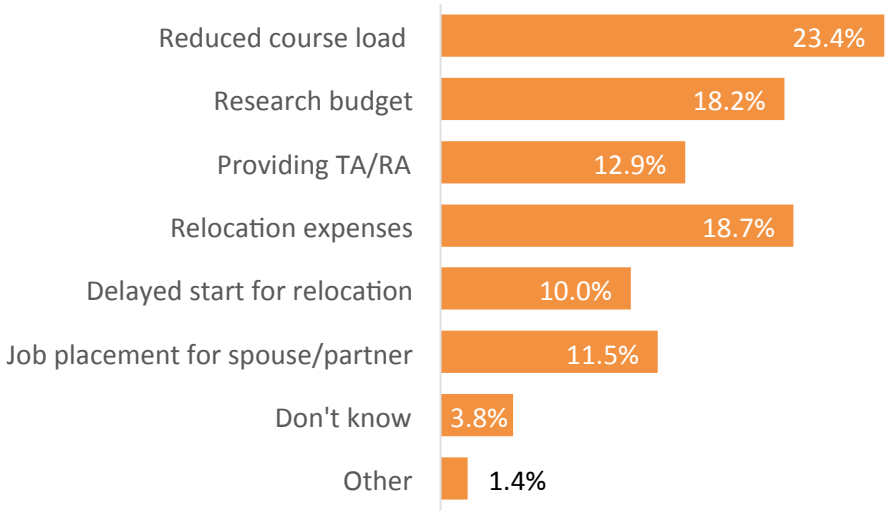


Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=104 with 5 missing and 11 responding "Not Applicable".
Due to round-off errors, the sum of the percentages may not be exactly 100%.

Finally, institutions may have more flexibility in offering non-pecuniary benefits that are a one-time offer to applicants rather than adjusting salaries which confer a permanent cost. This is particularly important when institutions are concerned with maintaining certain standards of equity across newly recruited versus current faculty, who may be paid less than the starting salary needed to attract candidates. Figure 19 reports the frequency with which 4-Year CAE institutions offer various incentives when hiring cybersecurity faculty. Note that the response rate among CAE-2Y institutions was too low to be able to make meaningful inferences about the

use of these incentives.[5] Among 4-Year CAE institutions, reduced course load was the most commonly used incentive (23.4 percent) followed closely by relocation expenses (18.7 percent) and providing additional funding for travel and research (18.2 percent). Institutions offering to help an applicant's spouse or significant other to find a job was also a somewhat frequent response (11.5 percent) among the other institutional offerings.

Figure 19: Percent of Respondents Indicating Special Incentives Offered to Cybersecurity Applicants, 4-Year CAE Institutions



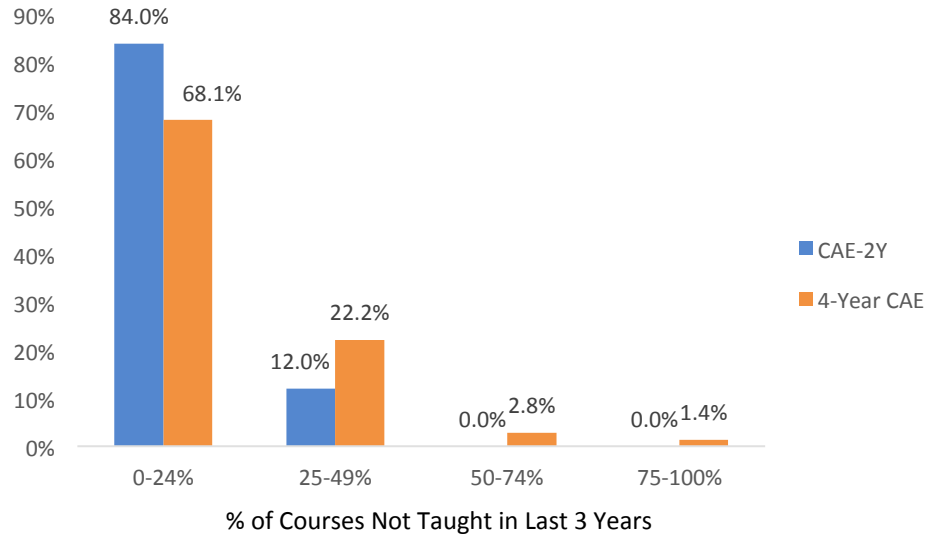
Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Respondents could choose more than one option. Due to round-off errors, the sum of the percentages may not be exactly 100%.

Unfortunately, the primary non-pecuniary incentive offered is for faculty to do less teaching. While this may be an effective incentive to hiring more faculty in the short-run, it contributes to the lack of teaching capacity at 4-Year CAE institutions. To determine the impact that the cybersecurity faculty shortage is having on teaching capacity, we asked respondents to indicate the percent of their institution's cybersecurity course catalog not being offered in the last three years due to the lack of a qualified instructor. Figure 20 shows that the majority of respondents at both types of institutions indicated that less than a quarter of courses were

[5] Unfortunately, the response set for this question from CAE-2Y institutions was very limited, with only 31 total responses, of which 14 responded ""Not Applicable"." The remaining 16 responses cited reduced course load as the most frequent incentive (5), followed by "don't know" (4) and "additional research and/or travel budget" (3).

affected by the lack of qualified instructors. However, 12.0 percent of CAE-2Y and 22.2 percent of 4-Year CAE indicated that between one-quarter to one-half of the courses in their catalog had not been taught in the past three years due to a lack of cybersecurity faculty. The higher share of 4-Year CAE institutions reporting this as an issue may be linked to the course buyouts offered to new hires.

Figure 20: Distribution of Percent of Courses Not Taught in Last 3 Years Due to Lack of Qualified Instructors, by CAE Designation



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=92 with 6 missing and 17 responding "Not Applicable" and 5 "Don't know". Due to round-off errors, the sum of the percentages may not be exactly 100%.

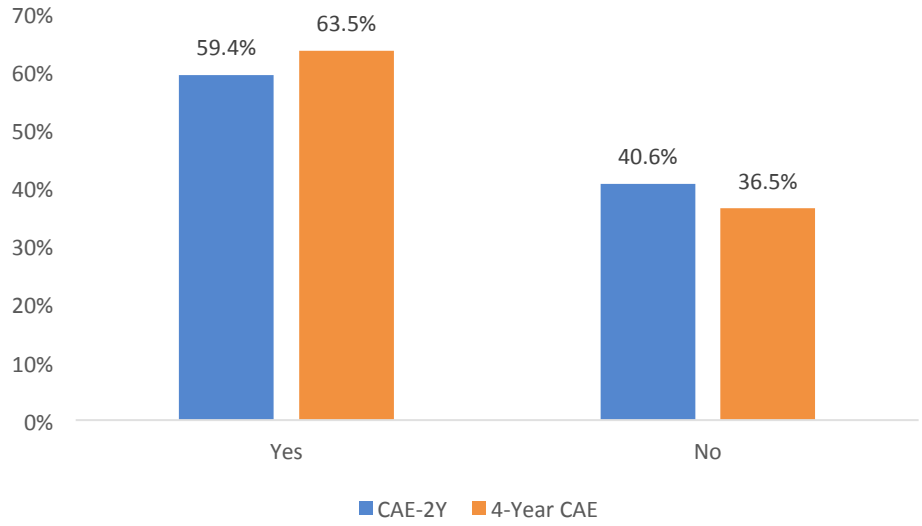
F. Current Pipeline of Potential Cybersecurity Faculty

Higher education institutions not only employ new cybersecurity faculty but also produce them as well. The last section of our survey focused on the current pipeline of potential cybersecurity faculty by asking respondents about the degrees they offer, the courses they teach, and which sectors their students are likely to pursue upon graduation (e.g. private sector, academia, or government).

Although cybersecurity is a field in high demand, Figure 21 shows that only about 60 percent of CAE institutions offer a specialized cybersecurity degree program. It may be the case

that the lack of a specialized degree program could play a role in producing an insufficient number of faculty to design and to develop the required curriculum.

Figure 21: Percent of Institutions Offering a Specialized Cybersecurity Degree, by CAE Designation



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=117 with 3 missing.

Interestingly, which department offers a specialized cybersecurity degree program differs considerably by institution. Table 10 shows that among CAE-2Y institutions, such programs are overwhelmingly offered by IT departments (70.0 percent) followed by Computer Science departments (20 percent). The emphasis on IT could reflect the more applied nature of CAE-2Y programs that often offer certificates as well as Associate's degrees. In contrast, there is a greater diversity of departments offering cybersecurity degrees among the 4-Year CAE institutions. The most prevalent department is Computer Science (40.8 percent) followed by IT (27.6 percent). However, a variety of other departments such as Business, Engineering, and Policy or Political Science also house cybersecurity degree programs. It may be the case that the choice of department at 4-Year CAE programs depends on the emphasis of the program (e.g. technical versus non-technical) or the availability of resources, particularly if cybersecurity faculty are able to command high salaries.

Table 10: Distribution of Departments Offering a Specialized Cybersecurity Degree, by CAE Designation

	CAE-2Y		4-Year CAE	
Department Name	**Count**	**Percent**	**Count**	**Percent**
Information Technology (or similar)	14	70.0%	21	27.6%
Computer Science	4	20.0%	31	40.8%
Other	2	10.0%	8	10.5%
Business School	0	0.0%	7	9.2%
Electrical and Computer Engineering	0	0.0%	3	4.0%
Electrical Engineering	0	0.0%	2	2.6%
Policy or Political Science	0	0.0%	2	2.6%
Combined Computer Science and Electrical Engineering	0	0.0%	1	1.3%
Law School	0	0.0%	1	1.3%
Don't know	0	0.0%	0	0.0%
(Total)	20	100.0%	76	100.0%

Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=97 with 22 missing and 1 responding "Not Applicable".
Due to round-off errors, the sum of the percentages may not be exactly 100%.

The distribution of cybersecurity course offerings was quite similar at both types of institutions. Table 11 shows that the most prevalent courses included network security, digital forensics, overview of IA or cybersecurity, and intrusion detection with more than 10 percent of institutions offering such courses. Other courses that were frequently offered between 5 to 10 percent of the time included policy and legal, penetration or capture the flag, cryptography theory, secure system design, applied cryptography, and malware analysis.

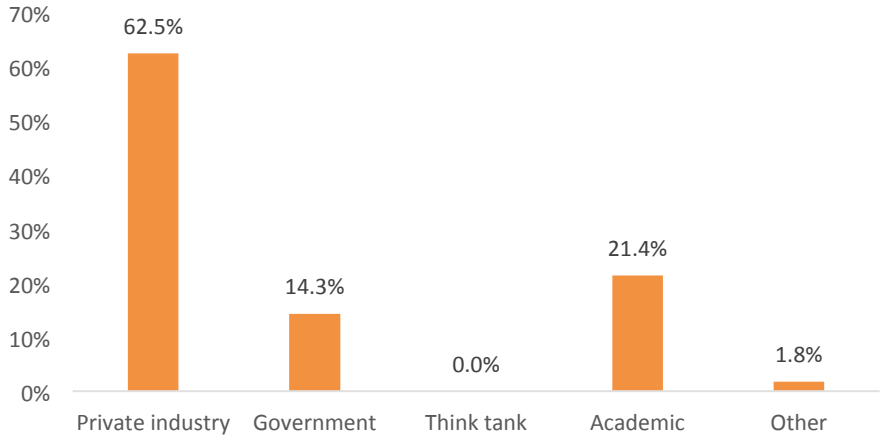
Table 11: Distribution of Cybersecurity Course Offerings, by CAE Designation

	CAE-2Y		4-Year CAE	
Cybersecurity Course/Topic	**Count**	**Percent**	**Count**	**Percent**
Network Security	31	14.0%	83	12.4%
Digital Forensics	29	13.1%	67	10.0%
Overview of IA or CySec	28	12.7%	76	11.4%
Intrusion Detection	25	11.3%	61	9.1%
Policy and Legal	24	10.9%	65	9.7%
Penetration, Capture the Flag	22	10.0%	59	8.8%
Cryptography Theory	18	8.1%	65	9.7%
Secure System Design	18	8.1%	59	8.8%
Applied Cryptography	11	5.0%	60	9.0%
Malware Analysis	11	5.0%	41	6.1%
Reverse Engineering	4	1.8%	29	4.3%
Other	0	0.0%	4	0.6%
(Total)	221	100.0%	669	100.0%

Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Respondents could choose multiple options. Due to round-off errors, the sum of the percentages may not be exactly 100%.

Finally, to get some insight into how leaky the pipeline is for new cybersecurity faculty, we asked 4-Year CAE respondents to indicate where they thought their Ph.D. students were most interested in working after they completed their degrees. Consistent with the previous findings of losing cybersecurity applicants to the private sector, Figure 22 indicates that respondents overwhelming felt their institution's Ph.D. students were most interested in working in private industry (63 percent), followed by academia (21 percent), and government (14 percent). Compared to previous research, which found that roughly one-third of doctoral recipients chose to enter academia in 2015, our findings indicate that the cybersecurity pipeline may be leaking even though more candidates have been graduating in recent years, as the private sector job market continues to strengthen in the wake of the Great Recession.

Figure 22: Distribution of Sectors Doctoral Recipients are Likely to Pursue, 4-Year CAE Institutions



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=56 with 4 missing and 24 responding "Not Applicable".

IV. Conclusion

Growing threats posed by both cybercriminals and hostile nation states have significantly increased demand for cybersecurity personnel in the U.S., both in the government sector as well as the private sector (DoD 2013). Yet, there is evidence that the need for cybersecurity personnel may be outstripping the educational establishment's ability to produce them (BGT 2015). Moreover, the high demand for cybersecurity workers is unlikely to be met by short-term training solutions, but rather are likely to require greater capacity and coordination with higher education institutions with more than 80 percent of cybersecurity job postings requiring at least a bachelor's degree and/or at least three years of experience.

Although the government has developed programs to develop standardized cybersecurity training and attract more students into the field, the growth in demand for cybersecurity education has yielded a shortage of qualified cybersecurity *educators*. The current production of doctoral recipients in cybersecurity-related disciplines appears insufficient to meet demand for such educators. To determine the magnitude of the problem as well as its potential causes, we developed and administered an online survey instrument to liaisons at educational institutions belonging to the NSA/DHS Centers of Academic Excellence (CAE). The survey focused on the characteristics of current faculty, challenges in the recruitment of new cybersecurity faculty, and the impact of the faculty shortage on the number of cybersecurity courses offered.

The results from our survey indicate that a significant number of CAE institutions have difficulty filling faculty positions. Almost half of CAE-2Y and about one-third of 4-Year CAE respondents indicated that their institution currently had a vacancy. Despite using a variety of recruiting channels, 4-Year CAE institutions tend to have vacancies that are open for long durations—often one to two years. As a result, most institutions need to conduct multiple searches to fill a position. For example, among 4-Year CAE institutions, only 37.5 percent respondents indicated that they were able to fill a cybersecurity position from just one search. Another 30.0 percent required two searches and 20.0 percent required three or more searches.

One reason for the difficulty in recruitment is the lack of qualified applicants with one in five CAE-2Y institutions and one in seven 4-Year CAE institutions report receiving zero qualified candidates. In addition, over half of CAE-2Y institutions report that the number of

qualified candidates that they are seeing has decreased over the past three years. Although upwards of one-quarter of CAE-2Y respondents indicated that they had raised either education or experience requirements, their institutions were willing to be flexible in terms of the required qualifications to be able to fill the position. Alternatively, 4-Year CAE institutions reported that non-citizens were either "very important" or "important" as a potential source of faculty. Providing CAE-2Y institutions with greater resources to recruit non-citizens could expand the pool to qualified candidates.

According to our survey, one of the main reasons why CAE institutions have difficulty hiring faculty is that they are often competing with the private sector. This is particularly true for CAE-2Y institutions that value practical, hands-on experience with upwards of 84 percent requiring some experience, most frequently in the range of 2-5 years although not necessarily in cybersecurity. Both CAE-2Y and 4-Year CAE institutions cited losing candidates to the private sector as one of the top factors in failed searches. Not surprisingly, over half of 4-Year CAE institutions and more than 70 percent of CAE-2Y reported that the salary offered by their institutions was "very often" or "often" cited by candidates as too low or not competitive. In addition to losing candidates, most CAE institutions have lost at least one faculty member over the past three years, often to the private sector. Finally, only 20 percent of doctoral recipients from 4-Year CAE institutions are seeking to enter academia upon graduation—further indication that the current faculty shortage is likely to continue for the foreseeable future without some type of policy intervention.

While it is not always possible for institutions to offer a competitive salary that will attract full-time tenure-track faculty, with additional funding it may be possible to attract candidates that are on the margin. For example, in New York State, the SUNY High Needs competitive grant program helps fund academic programs such as agriculture, biomedical, engineering, finance, healthcare, information technology, public health, and renewable/clean energy—programs that connect directly to specific workforce needs and whose graduates would fill jobs in high demand in New York State.[6] Similar programs have operated at the federal level to help fund nursing programs that face faculty shortages similar to those found in cybersecurity

[6] See http://system.suny.edu/academic-affairs/acaproplan/high-needs/ for more details on the SUNY High Need program.

(Aiken, Cheung, & Olds 2009). One could design such a competitive U.S. Government grant program to provide an extra stipend for up to two years for newly recruited cybersecurity faculty at CAE and other institutions [1] as a way to incentivize more faculty candidates to choose academia over the private sector.

Although CAE institutions have difficulty competing with the private sector on salary to be able to attract candidates, they do offer other benefits to faculty. Among non-pecuniary benefits offered by 4-Year CAE institutions to attract candidates, reduced course load was the most commonly used incentive (23.4 percent) followed closely by relocation expenses (18.7 percent) and providing additional funding for travel and research (18.2 percent). Course releases at 4-year institutions allow new faculty members to build up their research programs. Similar benefits could be designed at CAE-2Y, allowing faculty members to strengthen their cybersecurity expertise. For example, faculty members could be allowed to work one day per week in cyber defense-relevant private sector positions, thereby gaining real-life experience in cyber defense while supplementing their incomes. More awareness of other benefits such as retirement and healthcare—which are often more generous at public institutions than those offered by the private sector—could also be helpful in boosting faculty recruitment.

According to our survey, CAE institutions have been filling teaching gaps with adjunct faculty and part-time instructors, thus enabling them to offer necessary cybersecurity courses of sufficient breadth and depth with the regularity required for students to complete their degrees on time. While some amount of adjunct faculty is desirable to bring in practical applications from the private sector or to provide flexibility when enrollments fluctuate, currently there appears to be an imbalance: less than 40 percent of faculty at CAE-2Y hold a full-time tenure track position and just over 50 percent of 4-Year CAE faculty fall into this category. Heavy dependence on adjunct faculty can limit a program's ability to further design and develop a coherent program of courses in a fast moving field, such as cybersecurity. It may be possible to convert some part-time faculty to full-time positions using a competitive grant program such as that described above.

The lack of cybersecurity faculty has real consequences for the nation's ability to produce more cybersecurity workers. Roughly 12.0 percent of CAE-2Y and 22.2 percent of 4-Year CAE respondents indicated that between one-quarter to one-half of the courses in their catalog had not

been taught in the past three years, due to a lack of cybersecurity faculty. As a result, only 60 percent of CAE institutions have a specialized degree program in cybersecurity, indicating a potential lack of capacity. Although adjunct faculty and distance learning may help address some of these course constraints, the lack of full-time faculty also limits the ability of departments to engage in curriculum design, provide sufficient student advising, and undertake new research. And finally, although only 10-15 percent of current cybersecurity faculty are eligible to retire, that percentage is likely to rise over the next decade, as the Baby Boom generation begins to retire in greater numbers—exacerbating the faculty shortage and further constraining the nation's ability to build a strong cybersecurity workforce.

This report is the first part of a larger study that aims to advise NSA on ways to address the cybersecurity faculty shortage. In this report, we discuss the findings of the survey including where the critical needs are, the degree of difficulty in finding qualified instructors, and the specific impediments to recruiting and retaining faculty at both 2 and 4 year institutions. In future work we will conduct an industry survey to discuss ways that industry and academe can collaborate to meet the need for qualified cybersecurity instructors. At the end of the larger study, we will conclude with recommendations for programs that the government can develop with the help of the private sectors to address the shortage of cybersecurity faculty and workers.

V. References

Aiken, L.H., Cheung, R.B., & Olds, D.M. 2009. "Education Policy Initiatives to Address the Nurse Shortage in the United States." *Health Affairs*, 28(4): w646–w656.

Burning Glass Technologies. 2015. "Cybersecurity jobs, 2015." http://burning-glass.com/research/cybersecurity

Department of Defense. 2013. "DoD cyber workforce strategy." http://dodcio.defense.gov/Portals/0/Documents/DoD

Lewis, C.E. 2017. "Analysis of Current and Future Computer Science Faculty Needs via Advertised Faculty Searches for 2017."http://web.cs.wpi.edu/~cew/papers/CSareas17.pdf

National Institute for Standards and Technology. 2016. "Draft NIST Special Publication 800-181, the NICE cybersecurity workforce framework (November 2016)," https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

Robert Rich, "The Great Recession: December 2007-June 2009, Federal Reserve History, 22 November 2013, https://www.federalreservehistory.org/essays/great_recession_of_200709

U. S. Congress. 2014. "Homeland Security Cybersecurity Boots-on-the-Ground Act." http://www.gpo.gov/fdsys/pkg/BILLS-113hr3107rfs/pdf/BILLS-113hr3107rfs.pdf

Zweben, S. and B. Bizot. 2016. "2015 Taulbee survey. Continued Booming Undergraduate CS Enrollment; Doctoral Degree Production Dips Slightly." Computing Research News, 28 (5).

VI. Appendix: Online Survey Instrument

Cybersecurity Survey 2017

As part of a project for the National Security Agency, a team of researchers led by Northeastern University is collecting information on the magnitude of the assumed shortage of qualified educators in cybersecurity among higher education institutions. To achieve this goal, we are conducting an online survey of all Centers of Academic Excellence to gather information that can be used to identify areas of critical need, impediments to finding qualified instructors, and potential solutions.

This survey will take approximately 20 minutes to complete. The questions will focus on your institution's experience with hiring, training and retaining faculty in cybersecurity over the past several years. This includes number of current cybersecurity faculty as well as the number of open cybersecurity positions and available candidates. Note that the term cybersecurity in this survey is inclusive of all related fields and degree types.

All data will be kept confidential and no data identifying institutions or individuals, either directly or indirectly, will be published or released. Please be sure to read the informed consent on the initial landing page before completing the survey. By completing this survey, you will be credited with outreach service in the CAE program.

Survey Sections

I. Characteristics of Current Cybersecurity Faculty
   A. Institutional Characteristics
   B. Faculty Characteristics

II. Recruitment of New Cybersecurity Faculty
   A. Required Qualifications
   B. Recruiting Practices
   C. Applicant Pool

III. Cybersecurity Degree Programs and Courses Offered
   A. Degree Programs
   B. Courses Offered

I. Characteristics of Institution and Current Cybersecurity Faculty

A. Institutional Characteristics

1. Please indicate which of the following NSA/DHS Center of Academic Excellence designations have been awarded to your institution. (check all that apply)
CAE – 2Y
CAE – CD
CAE – R
CAE – CO

2. What is the type of your institution?
2 year public
2 year private
4 year public
4 year private
Other (please specify) _____

3. What is the highest degree conferred at your institution?
Associate's degree
Bachelor's degree
Master's or professional degree (MA, MBA, JD, MD)
Ph.D.

4. Approximately, how many students attend your institution?
Fewer than 1000
1,000 - 2,499
2,500 - 4,999
5,000 - 9,999
10,000 +

5. What is the zip code of your main campus?

_____

6. Is your institution located near (e.g. in the same county as) a government cybersecurity research laboratory or operational center?
Yes
No
Don't know

7. Is your institution located near (e.g. in the same county as) a large employer of cybersecurity workers?
Yes
No

Don't know

B. Characteristics of Current Cybersecurity Faculty

8. What is the name of the department in which the majority of your current cybersecurity faculty have their appointment? (If faculty are equally spread across multiple departments, please list all of those departments here.)

_____

9. How many of the cybersecurity faculty at your institution are in the following categories?

Full-time tenure-track _____
Part-time tenure-track _____
Full-time non-tenure track _____
Part-time non-tenure track _____
Don't know _____

10. How many of the cybersecurity faculty at your institution have the following title?

Adjunct _____
Instructor _____
Lecturer _____
Research faculty _____
Teaching faculty _____
Assistant professor _____
Associate professor _____
Full professor _____
Chaired professor _____
Don't know _____

11. How many of the cybersecurity faculty at your institution have the following qualifications?

Bachelor's degree _____
Bachelor's degree plus 2 or more years work experience in cybersecurity _____
Master's degree _____
Master's degree plus 2 or more years work experience in cybersecurity _____
Doctorate degree _____
Doctorate degree plus 2 or more years work experience in cybersecurity _____
Don't know

12. How many of the cybersecurity faculty at your institution have their primary degree in the following fields?

Cybersecurity _____
Computer science _____
Computer engineering _____
Information technology _____
Mathematics _____

Law _____
Criminal Justice _____
Business _____
Don't know
Other (please specify) _____

13. Are tenured or tenure-track cybersecurity faculty members expected to provide for their own summer salaries, either through research activities or additional teaching?
Yes
No
Don't know
"Not Applicable"

14. What percentage of current cybersecurity faculty use the following activities to supplement their academic salaries?
Teaching additional courses beyond required load _____
Cybersecurity consulting, personal business _____
Cybersecurity consulting, industry _____
Externally funded projects _____
Don't know
"Not Applicable"
Other (please specify) _____

15. How many cybersecurity faculty members have left your institution in the past 3 years?

_____

16. Please indicate the primary reason(s) why cybersecurity faculty have left your institution (check all that apply)
Hired by other institutions of higher education
Hired by private industry
Hired by government
Retirement
Don't know
"Not Applicable"
Other (please specify) _____

17. How many retirement-eligible faculty members are currently teaching cybersecurity courses at your institution?

_____

II. Recruitment of New Cybersecurity Faculty

A. Required Qualifications

18. Which governing body sets the minimum qualifications for cybersecurity faculty positions at your institution?
Local control
State control
National (e.g. industry) organization
Accrediting body
Don't know
"Not Applicable"
Other (please specify) _____

19. Please indicate the MINIMUM degree requirements for cybersecurity faculty positions required by your institution.
Bachelor's degree
Master's degree
Doctorate
Don't know
"Not Applicable"

20. Over the past five years, how have the MINIMUM degree requirements for cybersecurity positions CHANGED at your institution when posting a vacancy?
Increased
Decreased
Stayed the same
Don't know
"Not Applicable"

21. Please indicate the MINIMUM work experience requirements for cybersecurity faculty positions required by your institution.
None
Some work experience in cybersecurity but less than one year
At least one year work experience in cybersecurity but less than two years
At least two years work experience in cybersecurity but less than five years
Five or more years work experience in cybersecurity
Some work experience but NOT necessarily in cybersecurity
Don't know
"Not Applicable"

22. Over the past five years, how have the MINIMUM work experience requirements for cybersecurity positions CHANGED at your institution when posting a vacancy?
Increased
Decreased

Stayed the same
Don't know
"Not Applicable"

23. How often has your institution made exceptions to the typical minimum qualifications to recruit cybersecurity faculty because of recruiting difficulties?
Very often
Often
Sometimes
Rarely
Never
Don't know
"Not Applicable"

24. In your experience/opinion, for which of the following categories is it more difficult to recruit cybersecurity faculty at your institution?
Practitioners (e.g., holders of advanced certifications)
Traditional degree holders (e.g., Master's or PhD degrees)
Equally difficult
Don't know
"Not Applicable"
Other (please specify) _____

25. In your experience/opinion, for which of the following fields is it more difficult to recruit cybersecurity faculty at your institution?
Technical (e.g. computer science, computer engineering, information technology, mathematics)
Non-technical (e.g., law, criminal justice, business)
Equally difficult
Don't know
"Not Applicable"
Other (please specify) _____

26. In your experience/opinion, how important is it to be able to recruit individuals who are neither citizens nor permanent residents as a source of cybersecurity faculty at your institution?
Very important
Important
Somewhat important
Not Important
Don't know
"Not Applicable"

B. Recruiting Practices

27. Which of the following channels does your institution typically use to advertise for cybersecurity positions (check all that apply)?
Post vacancy on institution's public web site
Post vacancy on a job board web site
Post vacancy through an industry web site or publication
Post vacancy through an education web site or publication (e.g. Chronicles of Higher Education)
Post on social media web site (e.g. LinkedIn, Facebook, Twitter)
Ask faculty for referrals
Use a headhunter
Don't know
"Not Applicable"
Other (please specify) _____

28. For each of the following categories, how many open positions (new or vacant) for cybersecurity faculty do you currently have or expect to have at your institution over the next year?

Full-time tenure-track	_____
Part-time tenure-track	_____
Full-time non-tenure track	_____
Part-time non-tenure track	_____
Research faculty	_____
Teaching faculty	_____
Instructor	_____
Adjunct	_____
Don't know	_____
"Not Applicable"	

29. If you have any positions currently open, what is the expected level at which you intend to fill this cybersecurity position (check all that apply)?

	Junior/Untenured	Senior/Tenured	Any Level
Full-time tenure-track	_____	_____	_____
Full-time non-tenure track	_____	_____	_____
Part-time tenure-track	_____	_____	_____
Part-time non-tenure track	_____	_____	_____
Research faculty	_____	_____	_____
Teaching faculty	_____	_____	_____
Adjunct	_____	_____	_____
Instructor	_____	_____	_____
Lecturer	_____	_____	_____

30. If you have any positions currently open, how many months has the current cybersecurity position (new or vacant) been open for each of the following categories?
Full-time tenure-track _____

Full-time non-tenure track _____
Part-time tenure-track _____
Part-time non-tenure track _____
Research faculty _____
Teaching faculty _____
Instructor _____
Adjunct _____
Don't know
"Not Applicable"

31. If you currently have an open position, please list the website address of the posting (e.g. institution website/job board):

C. Applicant Pool

32. For each type of position, approximately how many qualified cybersecurity candidates typically apply to your institution's job posting?

Full-time tenure-track _____
Full-time non-tenure track _____
Part-time tenure-track _____
Part-time non-tenure track _____
Research faculty _____
Teaching faculty _____
Instructor _____
Adjunct _____
Don't know
"Not Applicable"

33. How has the number of qualified applicants for cybersecurity positions changed over the last three years?

Increased
Decreased
Stayed the same
Don't know
"Not Applicable"

34. For each type of position, approximately how many cybersecurity candidates did your institution successfully recruit?

Full-time tenure-track _____
Full-time non-tenure track _____
Part-time tenure-track _____
Part-time non-tenure track _____

Research faculty _____
Teaching faculty _____
Instructor _____
Adjunct _____
Don't know
"Not Applicable"

35. Please indicate the number of searches that your institution typically conducts before finding a qualified candidate.
One search
Two searches
Three searches
Four searches
Five searches
More than five searches
Search is still ongoing
Don't know
"Not Applicable"

36. If your department has been unsuccessful in recruiting cybersecurity candidates, please indicate the primary reasons why (rank the top three).
Candidates chose a better position at another academic institution
Candidates chose a better position from the private sector
Candidates chose a better position from the government sector
Candidates chose another position near their spouse/partner/significant other
Candidates chose to stay at their current institution
Candidates chose to pursue a post-doc instead
Candidates cited the balance of teaching to research at our institution as unattractive
Candidates cited the class sizes at our institution as unattractive
Candidates cited the number of "advanced" students at our institution to be unattractive
Candidates cited the salaries at our institution to be too low or not competitive
Our department chose not to make an offer because the candidates were not qualified
Don't know
"Not Applicable"
Other (please specify) _____

37. How often do cybersecurity candidates cite that the salary is too low or not competitive with other positions when rejecting a job offer from your institution?
Very often
Often
Sometimes
Rarely
Never
Don't know
"Not Applicable"

38. For which types of positions have cybersecurity candidates cited that the salary is too low or not competitive with other positions when rejecting a job offer from your institution (check all that apply)?

Full-time tenure-track _____
Full-time non-tenure track _____
Part-time tenure-track _____
Part-time non-tenure track _____
Research faculty _____
Teaching faculty _____
Instructor _____
Adjunct _____
Don't know
"Not Applicable"

39. In your opinion, how supportive is the administration at your institution regarding the recruitment of new cybersecurity faculty?

Very supportive
Supportive
Somewhat supportive
Unsupportive
Not supportive at all
Don't know
"Not Applicable"
Prefer not to answer

40. Has your institution offered any of the following special incentives for hiring cybersecurity faculty? (Check all that apply).

Reduced course load for the first few semesters
Additional research or travel budget
Providing a teaching or research assistant
Paying relocation expenses
Delayed start date to accommodate relocation
Help with finding employment for spouse or significant other
Don't know
"Not Applicable"
Other: _____

41. What are the primary sources for hiring ADJUNCT cybersecurity faculty at your institution? (rank the top three)

Individuals from industry who teach during non-work hours
Individual from government labs or other government organizations who teach during non-work hours
Individuals who teach at multiple institutions as an adjunct
Graduate students from other institutions

Semi-retired individuals
Don't know
"Not Applicable"
Other (please specify) _____

42. Please indicate the primary motivation why ADJUNCT cybersecurity instructors choose to teach at your institution (rank the top three):

To earn extra compensation ____
To earn Continuing Education Credits (CEU's) to maintain certifications ____
Because of a sense of civic duty or patriotism ____
Because they enjoy teaching ____
As a way to transition to a career in academia ____
To recruit future colleagues ____
Don't know
"Not Applicable"
Other (please specify) _____

<u>Other Qualifications (to be Asked of 2 Year Institutions Only)</u>

i. What is the minimum level of teaching experience required by your institution?

Part time community college
Full time community college
Part time four year institutions
Four year lecturer
Full time four year institutions
Don't know
"Not Applicable"
Other (please specify) _____

ii. Does your institution require that faculty be capable to teach all courses in the discipline for which they are hired?

Yes required
No, preferred
Don't know
"Not Applicable"

iii What type of curriculum development experience does your institution require? (check all that apply)

None
Occasional course
Program, degree and/or certificate development
Served on local curriculum committee
Served on state level curriculum committee
Don't know
"Not Applicable"

Other (please specify) _____

iv. What area of specialization is your institution most interested in with regards to hiring cybersecurity faculty? (check all that apply)

	Introductory	Intermediate	Advanced
Fundamentals of Security	_____	_____	_____
Networking	_____	_____	_____
Systems	_____	_____	_____
Business Management	_____	_____	_____
Risk analysis/Auditing	_____	_____	_____
Legal/Policy	_____	_____	_____
Other			
Don't know			
"Not Applicable"			

v. What type of work experience is your institution most interested in with regards to hiring cybersecurity faculty? (check all that apply)?

Private industry
Government
Think tank
Academic
Don't know
"Not Applicable"
Other (please specify) _____

vi. Is your institution interested in hiring cybersecurity faculty that have experience with outreach activities to the K-12 institutions?

Yes
No
Don't know
"Not Applicable"

vii. Is your institution interested in hiring cybersecurity faculty with cyber competition experience?

Yes
No
Don't know
"Not Applicable"

III. Cybersecurity Degree Programs and Courses Offered

A. Degree Programs

43. Do you offer a specialized cybersecurity degree?
Yes
No
Don't know
44. Through what department is the specialized cybersecurity degree offered? (Check all that apply)
Information Technology (or similar)
Computer Science
Electrical Engineering
Electrical and Computer Engineering
Combined Computer Science and Electrical Engineering
Law School
Business School
Policy or Political Science
Other (please specify) _____
Don't know
"Not Applicable"

45. Please indicate how many students typically graduate *per year* from your institution with a cybersecurity degree or focus (e.g., thesis or dissertation) from each of the following programs:
Certificate _____
Associate _____
Bachelor _____
Masters _____
Ph.D. _____
Don't know
"Not Applicable"

46. Does your institution offer non-degree professional education in cybersecurity (e.g., short courses, certificates, or single courses)?
Yes
No
Don't know
"Not Applicable"

47. Does your institution offer distance learning in any of the following degree programs (check all that apply)?
Associate degree
Bachelor's degree
Master's degree
Ph.D.
Don't know
"Not Applicable"

B. Courses Offered and Taught

48. Does your institution offer cybersecurity courses covering the following topics (check all that apply)

Overview of IA or CySec
Cryptography theory
Applied Cryptography
Network Security
Malware Analysis
Reverse Engineering
Policy and Legal
Intrusion Detection
Digital Forensics
Secure system design
Penetration and capture the flag
Don't know
"Not Applicable"
Other (please specify) _____

49. Of the cybersecurity courses listed in your institution's catalog, what percentage are offered through the following degree programs?

	Undergraduate	Graduate	Certificate
0-24%	_____	_____	_____
25-49%	_____	_____	_____
50-74%	_____	_____	_____
75-99%	_____	_____	_____
100%	_____	_____	_____
Don't know			
"Not Applicable"			

50. Of the cybersecurity courses listed in your institution's catalog, what percentage are offered at the following difficulty levels?

	Introductory	Intermediate	Advanced
0-24%	_____	_____	_____
25-49%	_____	_____	_____
50-74%	_____	_____	_____
75-99%	_____	_____	_____
100%	_____	_____	_____
Don't know			
"Not Applicable"			

51. Indicate what percentage of your cybersecurity courses are taught by each of the following categories of instructors:

	Cybersecurity Faculty	**Faculty from Other Departments**	**Adjunct Instructors**	**Graduate Students**
0-24%	_____	_____	_____	_____
25-49%	_____	_____	_____	_____
50-74%	_____	_____	_____	_____
75-99%	_____	_____	_____	_____
100%	_____	_____	_____	_____
Don't know				
"Not Applicable"				

52. Of the cybersecurity courses listed in your institution's catalog, what percentage have NOT been taught in the last three years due to a lack of qualified instructors?

0-24%
25-49%
50-74%
75-99%
100%
Don't know
"Not Applicable"

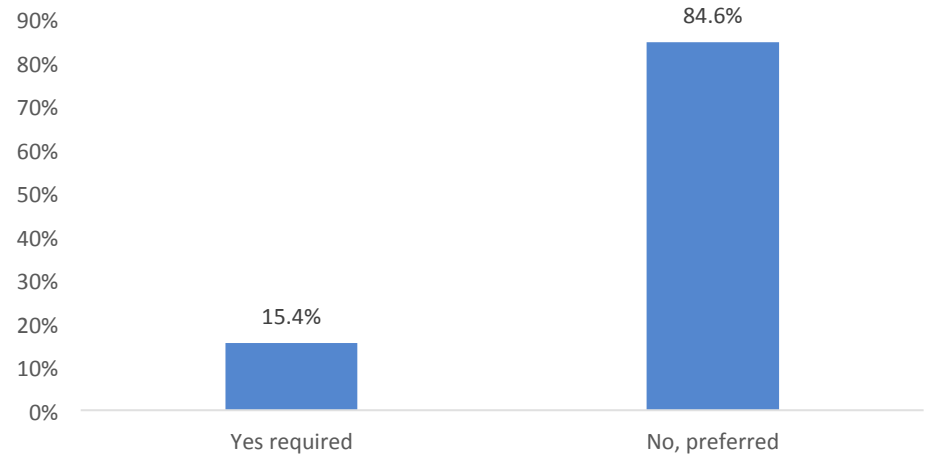
VII. Appendix B: Additional Results for CAE-2Y Institutions

Table B1: Distribution of Minimum Level of Teaching Experience Required CAE-2Y Only

Level	Count	Percent
Part time community college	10	35.7%
Full time community college	0	0.0%
Part time four year institutions	0	0.0%
Four year lecturer	0	0.0%
Full time four year institutions	0	0.0%
Don't know	6	21.4%
Not applicable	8	28.6%
Other	4	14.3%
(Total)	28	100.0%

Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=28.

Figure B1: Faculty Required to Teach All Courses in Their Hiring Discipline CAE-2Y Only



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=26 with 2 responding "Not Applicable."

Table B2: Distribution of Requirements for Curriculum Development Experience CAE-2Y Only

Experience Type	Count	Percent
None	11	29.7%
Occasional course	7	18.9%
Program, degree and/or certificate development	9	24.3%
Served on local curriculum committee	4	10.8%
Served on state level curriculum committee	2	5.4%
Don't know	2	5.4%
Other	2	5.4%
Total	37	100.0%

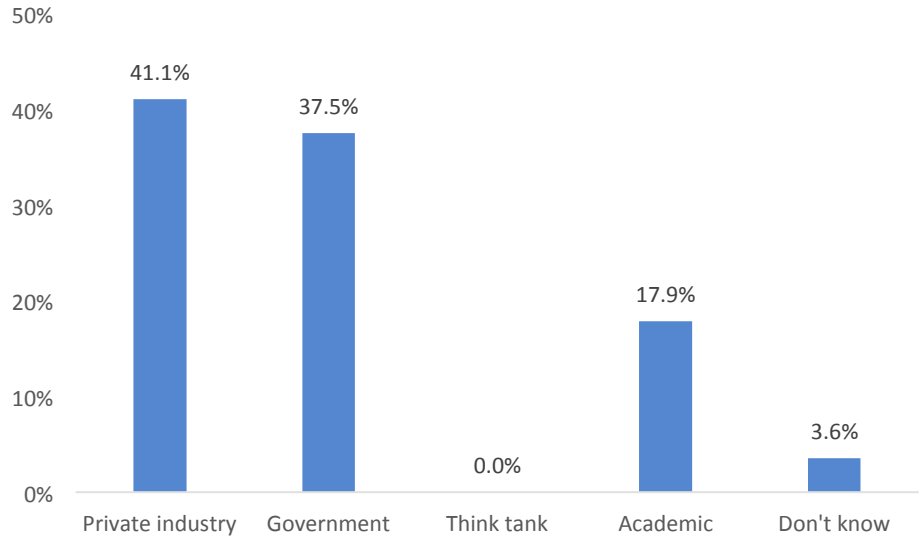
Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Respondents could choose more than one option.

Table B3: Distribution of Specializations Most Sought After by Institutions When Hiring CAE-2Y Only

Specialization	Introductory (Column %)	Intermediate (Column %)	Advanced (Column %)
Fundamentals of Security	28.1%	24.5%	32.0%
Networking	20.3%	34.7%	32.0%
Systems	15.6%	24.5%	12.0%
Business Management	6.3%	4.1%	4.0%
Risk analysis/Auditing	15.6%	6.1%	4.0%
Legal/Policy	10.9%	2.0%	4.0%
Other	1.6%	2.0%	8.0%
Don't know	0.0%	0.0%	0.0%
Not applicable	1.6%	2.0%	4.0%
(Total)	100.0%	100.0%	100.0%
(Total Count)	64	49	25

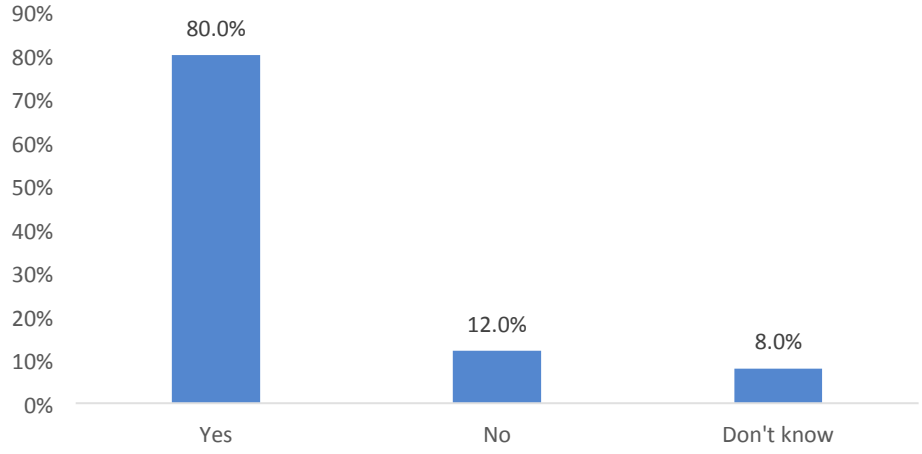
Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Respondents could choose more than one option.

Figure B2: Type of Work Experience Sought by Institutions CAE-2Y Only



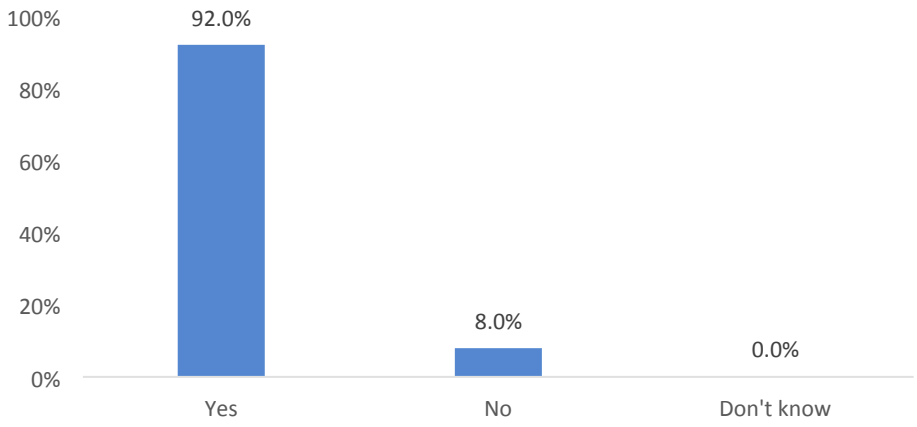
Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Respondents could choose more than one option.

Figure B3: Preference for Faculty with K-12 Institutional Outreach Activity Experience CAE-2Y Only



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=25 with 3 responding "Not Applicable."

Figure B4: Preference for Faculty with Cyber Competition Experience
CAE-2Y Only



Source: Authors' calculations from the 2017 CAE Member Institution Cybersecurity Survey.
Note: Number of respondents=25 with 3 responding "Not Applicable."