The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals

KEITH S. JONES, AKBAR SIAMI NAMIN, and MIRIAM E. ARMSTRONG,
Texas Tech University, Lubbock

Our cybersecurity workforce needs surpass our ability to meet them. These needs could be mitigated by developing relevant curricula that prioritize the knowledge, skills, and abilities (KSAs) most important to cybersecurity jobs. To identify the KSAs needed for performing cybersecurity jobs, we administered survey interviews to 44 cyber professionals at the premier hacker conferences Black Hat 2016 and DEF CON 24. Questions concerned 32 KSAs related to cyber defense. Participants rated how important each KSA was to their job and indicated where they had learned that KSA. Fifteen of these KSAs were rated as being of higher-than-neutral importance. Participants also answered open-ended questions meant to uncover additional KSAs that are important to cyber-defense work. Overall, the data suggest that KSAs related to networks, vulnerabilities, programming, and interpersonal communication should be prioritized in cybersecurity curricula.

CCS Concepts: • **Security and privacy**; • **Social and professional topics** → **Computing education**;

Additional Key Words and Phrases: Cyber-defense, cybersecurity education, cybersecurity curricula, knowledge, skills, and abilities, Cybersecurity Workforce Framework

ACM Reference format:
Keith S. Jones, Akbar Siami Namin, and Miriam E. Armstrong. 2018. The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals. *ACM Trans. Comput. Educ.* 18, 3, Article 11 (August 2018), 12 pages.
https://doi.org/10.1145/3152893

1 INTRODUCTION

Many of our day-to-day activities, such as communicating with others, conducting bank transactions and online purchases, and educating or entertaining ourselves, increasingly depend on the exchange of digital information. These activities are susceptible to cyber-attacks. Cybersecurity breaches are growing and are costly to the institutions attacked and to our national economy as a whole [1].

Thus, there is a growing need for educated and trained cybersecurity professionals who have the knowledge, skills, and abilities (KSAs) necessary to ensure that our exchanges of digital information are reliable and secure. Unfortunately, we do not have enough cyber attackers and defenders

This work is supported by the National Science Foundation under Award No. DGE-1516636.
Authors' addresses: K. S. Jones and M. E. Armstrong, Department of Psychological Sciences, Texas Tech University, Box 42051, Lubbock, TX 79409-2051; emails: {keith.s.jones, miriam.armstrong}@ttu.edu; A. S. Namin, Department of Computer Science, Texas Tech University, Box 43104, Lubbock, TX 79409-3104; email: akbar.namin@ttu.edu.

https://doi.org/10.1145/3152893

to meet our current security needs [2–4]. This talent shortfall has led to a call for more and better cybersecurity training curricula [3] so that attackers, defenders, and other members of the cybersecurity workforce will have the requisite KSAs for employment upon education and training completion and will not rely on on-the-job training [5].

1.1 Government Efforts to Promote Cyber Curricula

With the goal of supporting future cyber curricula efforts, the National Institute of Standards and Technology and the Department of Homeland Security (DHS) partnered to develop the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [6]. The intention of the NICE framework was to provide an overview of the work performed in the cybersecurity field. It outlines the relationship between different cybersecurity jobs and the KSAs used in each job type. The NICE framework identifies seven general knowledge areas corresponding to fields within cybersecurity (securely provision, operate and maintain, protect and defend, investigate, collect and operate, analyze, and oversee and govern). The protect and defend general knowledge area best exemplifies the cybersecurity skills in highest demand [2], and thus the KSAs within that knowledge area will be the focus of this project. Each general knowledge area contains two to seven specialty areas; within the protect and defend knowledge area, there are four specialty areas: (i) computer network defense analysis, (ii) computer network defense infrastructure support, (iii) incident response, and (iv) vulnerability assessment and management. The KSAs relevant to that job type are listed under each specialty area. For instance, 61 KSAs such as "Knowledge of basic system administration, network, and operating system hardening techniques" are listed under the computer network defense analysis specialty area. KSAs listed under each specialty area are not necessarily unique to that specialty area. All general knowledge areas, specialty areas, and KSAs can be found on the National Initiative for Cybersecurity Careers and Studies website [7].

Government efforts specific to increasing the number of cybersecurity training programs include the National Centers of Academic Excellence (CAE) designation provided on behalf of the National Security Administration (NSA) and the DHS [8]. Collegiate institutions may become a CAE when their curriculum covers a set of knowledge units (KUs) specified by the NSA and DHS. A KU may encompass multiple KSAs or may refer to a single concept that is somewhere between knowledge and a skill [9]. There are two CAE designations: Center of Academic Excellence in Cyber Defense (CAE-CD) and Center of Academic Excellence in Cyber Operations (CAE-CO). Requirements for the latter were based upon the findings of the NICE initiative [10]. That said, it is unclear which of the NICE framework's specialty areas or general knowledge areas the CAE-CO curriculum prepares students for. There is a cyber operations specialty area in the NICE framework (under the collect and operate general knowledge area), but it is impossible to compare the KUs of the CAE-CO program to the NICE cyber operations KSAs because they are not listed due to their highly specialized and classified nature [6–7]. There is no other specialty area that seems an obvious fit for a student educated through a CAE-CO program; it's possible that this type of curriculum is meant to provide a general education in cybersecurity and may not be appropriate for a program interested in supplying training for one general knowledge area within the NICE framework.

For curriculum developers interested in preparing future cyber attackers and defenders, these government initiatives leave two questions unanswered. First, how important is each KSA? Second, are existing cyber-security curricula adequately addressing the most important KSAs or must attackers and defenders seek further training post-graduation? Educators, especially those designing new courses, will not have unlimited time and energy to devote to teaching each of the 79 KSAs within the NICE protect and defend general knowledge area. Therefore, they must prioritize which KSAs to spend the most instruction time on. The NICE framework provides no prescriptive information about building a curriculum, and no indication of whether some KSAs are more critical

than others. The CAE guidelines are also unhelpful in answering this question. Again, there is no clear indication that a CAE curriculum would provide a strong educational foundation for a cyber attacker or defender. Furthermore, the CAE guidelines do require curriculum developers to choose between some of the KUs but without any means for prioritizing between them.

1.2 Academic Research on Cyber Curricula Development

The current literature on cybersecurity education also provides little guidance about what should be included in cyber defense curricula. An overview of curriculum development case studies indicates that course training requirements are based off of a variety of sources, including accreditation requirements [11–13], the needs of the local community [14], and KSAs that would theoretically benefit the field of cybersecurity [13, 15]. The authors have encountered no case studies in which curriculum requirements were based on employer demand, probably because there appear to be no academic investigations into what these demands are. Indeed, there is a need for industry input when designing security curricula [16].

There is also little academic study as to whether the KSAs being taught in existing cybersecurity programs match those demanded by the cybersecurity workforce. It is unlikely that graduates from CAE institutions are filling the demand that these programs are intended to address [17]. Such a demand gap may be due to inadequacies of the curricula, to a low number or cybersecurity programs overall [18], or some combination of the two. Current research does not indicate whether there are KSAs that are important to cyber attackers and defenders but are left out of current curricula.

1.3 Motivation of Present Study

The aim of the present study was to address the two limitations discussed above by providing direction for prioritizing KSAs in cyber curricula and by evaluating whether the most important KSAs are adequately covered by current education and training curricula.

To address the lack of direction for prioritizing KSAs in cyber curricula, we asked cybersecurity professionals to rate the importance of 32 KSAs related to cyber defense jobs. We focused on the KSAs within the NICE framework's protect and defend knowledge area and on professionals who worked within that field because it corresponded most closely with the intrusion detection and attack mitigation skills that are in critically short supply [2]. We also asked participants a series of open-ended questions concerning which programming languages, soft skills, and other skills are important to their cybersecurity work. This was intended to identify any KSAs that were outside of the purview of the NICE framework but nonetheless may be important to include in cyber curricula.

To determine whether these KSAs are currently being taught in cyber curricula, we asked professionals where they had learned each KSA. Additionally, we asked open-ended questions such as, "Was there anything you've had to learn on the job that you wish you had learned in school?" Overall, these questions were intended to assess gaps between cyber education and the KSAs required for cyber work and, therefore, provide another means by which to determine what should be included in cyber curricula.

2 METHODS

2.1 Procedure

Two researchers attended Black Hat USA 2016 and DEF CON 24. Both researchers followed the same procedure but worked independently. Researchers approached fellow conference attendees and asked them if they would be willing to participate in an interview to "help develop better

cyber training programs." Participation was voluntary and participants were told that they could skip any questions that they did not want to answer. Researchers read 81 questions (5 demographic questions, 64 NICE KSA questions, and 12 open-ended questions) aloud to the participants and then recorded participants' responses on paper. Researchers generally spent between 10 and 20 minutes with each participant.

2.2 Measures

Three main types of questions were asked during the interview: demographic questions, questions about 32 of the KSAs from the NICE framework's protect and defend general knowledge area, and general open-ended questions. Researchers also took notes on any additional comments volunteered by the participants (for example, many participants would explain why a particular KSA was important).

2.2.1 Demographic Questions. Participants were asked how many years they had been in cyber, how many capture-the-flag events they had participated in, what was the highest level of education completed, their major, and which of the four specialty areas under the NICE protect and defend knowledge area best described their job (computer network defense analysis, computer network defense infrastructure support, incident response, and vulnerability assessment and management [7]). We did not ask for more detailed information about the participant's employment or other personal information such as country of employment, as we were concerned that such questions would be interpreted as social engineering [19].

2.2.2 NICE KSA Questions. Participants answered questions regarding 32 of the KSAs from the NICE framework. The 32 KSAs were chosen because they were listed under two or more specialty areas within the framework's protect and defend general knowledge area. Therefore, it was assumed that these 32 KSAs would be the most important for cybersecurity attackers and defenders generally. The 32 KSAs used are listed in Table 1.

For each of the 32 NICE KSAs, participants were asked two questions. The first question was, "How important is [this KSA] for your job?" They rated each KSA on an anchored continuous rating scale of 1 to 6, with 1 being not at all important for the job and 6 being very important. The second question was, "Where did you learn [this KSA]?" If participants provided multiple answers, they were asked where they learned the most about the KSA. The answers provided fell into five categories: the KSA was learned at work/on the job, the KSA was learned at school, the KSA was learned through self-study, the KSA was learned someplace else (e.g., through government training, certification programs, or friends), or the KSA was not learned at all.

2.2.3 Open-Ended Questions. Open-ended questions were designed to capture cyber-related tools that could be taught in a cyber course or to uncover any KSAs relevant to cybersecurity professionals' jobs but that were not included in the NICE KSA lists. Participants were asked which tools they used for seven cybersecurity tasks: recovery, scanning or port scanning, intrusion detection, network traffic analysis, packet-level analysis, penetration testing, and network analysis. These questions were asked so that educators could make informed decisions about the tools used during hands-on learning activities. Researchers recorded all answers listed by the participants. To uncover KSAs that were not on the NICE lists, participants were asked to list all programming/scripting languages and all soft skills that were important to their jobs. For each, they rated how important the skill was on a scale of 1 to 6 and stated where they had learned that language or soft skill. To account for any additional KSAs that are important to cyber professionals, participants were asked questions such as, "What skills and topics that we haven't covered so far are most important to your job?"

Table 1. Results of the NICE KSA Questions

Knowledge, Skill, or Ability (KSA)	Importance to Job				Where the KSA Was Learned					
	n	*M* (*SD*)	*t*	*d*	*n*	job	school	self	other	n/a
1. How traffic flows across the network	43	5.14 (1.57)	6.860*	1.05	43	44.19	23.26	16.28	9.30	6.98
2. Network protocols	43	5.09 (1.48)	7.072*	1.08	43	48.84	27.91	16.28	2.33	4.65
3. System and application security threats and vulnerabilities	42	5.00 (1.29)	7.548*	1.16	42	52.38	9.52	28.57	7.14	2.38
4. Basic system administration, network, and operating system hardening techniques	44	4.95 (1.46)	6.599*	0.99	44	54.55	6.82	31.82	6.82	0.00
5. Network security architecture concepts	43	4.93 (1.40)	6.680*	1.02	43	44.19	32.56	11.63	4.65	6.98
6. General attack stages	43	4.91 (1.52)	6.051*	0.92	44	61.36	6.82	18.18	13.63	0.00
7. Different classes of attacks and recovery concepts and tools	42	4.86 (1.42)	6.176*	0.95	42	57.14	4.76	21.43	11.9	4.76
8. Recognizing and categorizing types of vulnerabilities and associated attacks	42	4.76 (1.53)	5.355*	0.83	41	70.73	2.44	19.51	4.88	2.44
9. Conducting vulnerability scans and recognizing vulnerabilities in security systems	41	4.76 (1.59)	5.048*	0.79	41	70.73	2.44	17.07	2.44	7.32
10. Computer network defense policies, procedures, and regulations	42	4.71 (1.50)	5.237*	0.81	43	55.81	11.63	23.26	6.98	2.33
11. Securing network communications	41	4.66 (1.74)	4.261*	0.67	41	63.41	9.76	12.20	2.44	12.20
12. Programming language structures and logic	42	4.62 (1.79)	4.043*	0.62	42	19.05	45.24	23.81	2.38	9.52
13. Information assurance principles and organizational requirements	43	4.60 (1.31)	5.522*	0.84	42	64.29	14.29	7.14	14.29	0.00
14. What constitutes a network attack and the relationship to both threats and vulnerabilities	41	4.59 (1.56)	4.441*	0.69	41	58.54	12.20	14.63	4.88	9.76
15. Network traffic analysis methods	43	4.44 (1.76)	3.502*	0.53	43	60.47	11.63	13.95	4.65	9.30
16. Using network analysis tools to identify vulnerabilities	43	4.42 (1.82)	3.318	0.51	42	61.90	7.14	16.67	4.76	9.52
17. Intrusion detection system tools and applications	43	4.33 (1.92)	2.814	0.43	41	58.54	4.88	19.51	4.88	12.20
18. Intrusion detection methodologies and techniques for detecting host and network-based intrusions	43	4.30 (1.88)	2.793	0.43	43	69.77	2.33	13.95	2.33	11.63
19. Performing packet-level analysis	42	4.29 (1.88)	2.712	0.42	42	52.38	11.90	16.67	7.14	11.90
20. Penetration testing principles, tools, and techniques	42	4.29 (1.93)	2.640	0.41	40	47.50	10.00	20.00	12.50	10.00
21. Incident response and handling methodologies	43	4.26 (1.83)	2.713	0.41	43	65.12	2.33	13.95	6.98	11.63
22. Host/network access controls	43	4.26 (1.87)	2.657	0.41	42	64.29	7.14	7.14	9.52	11.90
23. Different operational threat environments	43	4.16 (1.76)	2.472	0.38	42	57.14	9.52	11.90	11.90	9.52
24. Packet-level analysis	42	4.07 (1.80)	2.058	0.32	39	53.85	12.82	17.95	5.13	10.26
25. Detecting host and network-based intrusions	42	4.02 (1.96)	1.735	0.27	42	57.14	7.14	14.29	4.76	16.67
26. VPN security	42	4.00 (1.77)	1.834	0.28	42	50.00	7.14	16.67	4.76	21.43
27. Applying host/network access controls	42	3.90 (1.85)	1.421	0.22	42	57.14	9.52	11.90	4.76	16.67
28. Content development	42	3.86 (1.87)	1.239	0.19	41	48.78	21.95	14.63	0.00	14.63
29. Protecting a network against malware	42	3.86 (1.99)	1.160	0.18	42	59.52	4.76	11.90	2.38	21.43
30. Data backup, types of backups, and recovery concepts and tools	43	3.65 (1.63)	0.608	0.09	43	65.12	2.33	16.28	4.65	11.63
31. Using incident handling methodologies	43	3.63 (1.95)	0.430	0.07	43	48.84	9.30	16.28	4.65	20.93
32. Performing damage assessments	42	3.57 (1.93)	0.240	0.04	42	50.00	9.52	4.76	4.76	30.95

NICE KSAs are listed by mean importance rating, from highest to lowest. Some KSA names have been shortened for space; full names can be found on the NICE framework website (https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework). Listed under the Importance to Job column are number of respondents (*n*), mean (*M*), and standard deviation (*SD*) of the importance ratings for each NICE KSA. T values are the results of single-sample *t*-tests, and effect size (*d*) indicates the difference between *M* and a neutral importance rating expressed in terms of standard deviations. Listed under the Where the KSA Was Learned column are number of respondents (*n*) and the percentage of respondents who answered with: at work (job), through self-study (self), at school (school), somewhere else (other), or not learned at all (n/a).

*$p < 0.002$

2.3 Participants

Forty-four cyber professionals participated in this study. All were attendees at one or both of the premier hacking conferences Black Hat USA 2016 and DEF CON 24. Because a monetary compensation process would have required the collection of personal information (e.g., name, address) and because the researchers were led to believe that cyber professionals prefer to remain anonymous at these conferences [20], participants were not compensated for their time. Due to privacy concerns [19], we did not ask participants about their geographical location or current employment. While Black Hat and DEF CON are international conferences, they are consistently held in the United States. Furthermore, the participants who did voluntarily mention their employer worked for US companies or the US government. Therefore, it is reasonable to assume that the results of the survey pertain well to cybersecurity professionals in the United States but may not be internationally applicable.

On average, participants had been in cyber for 13.79 years ($SD = 8.83$; range: 1–34 years) and had participated in 3.95 capture-the-flag events ($SD = 6.26$; range: 0–30). Most participants (35) had completed some form of higher education (associate's, bachelor's, master's, etc.); 9 listed high school as their highest level of education. Of the 35 who completed some form of higher education, the most common majors listed were: computer science (10 respondents), computer engineering (3), information technology (2), math (2), and technical communications (2). The 16 other majors listed included fields commonly associated with computer science and engineering (e.g., electrical engineering, information security), and those rarely associated with technical fields (e.g., philosophy, theater).

Of the four specialty areas within the NICE framework's protect and defend general knowledge area, 7 respondents had jobs relating to computer network defense analysis, 10 related to computer network defense infrastructure support, 1 related to incident response, 18 related to vulnerability assessment and management, and 8 did not select one of the specialty areas as being relevant to their job.

3 RESULTS

3.1 What KSAs Are Most Important to Cybersecurity Professionals?

The mean importance ratings for all 32 NICE KSAs were above 3.5, which would be considered neutral on a 6-point continuous scale (Table 1). To test which KSAs should be most highly prioritized in course curricula, we performed a series of 32 t-tests. These tests compared the mean importance rating for each KSA against a neutral rating of 3.5 (the middle of the 1–6 importance scale). Fifteen of the KSAs were rated as being of significantly higher-than-neutral importance after a Bonferroni correction ($\alpha = .05/32 = .002$; Table 1). Single-sample t-tests are robust against violations of the normality assumption [21], and performing comparisons using the nonparametric Wilcoxon signed-ranks test provided the same outcomes as did the parametric t-test. Therefore, only the results of the t-tests are reported here.

Participants also listed and rated KSAs that were important to their jobs but not included in the NICE KSA lists. Participants gave 120 responses to the question, "What programing languages and scripts are important to your job?" Twenty-three unique programing/scripting languages were listed. The five most frequently listed languages accounted for 69% of responses and had a mean importance rating of 4.36 ($SD = 1.50$): Python ($N = 29, M = 4.5, SD = 1.57$), languages from the C family ($N = 19, M = 4.68, SD = 1.34$), Java ($N = 17, M = 4.76, SD = 1.11$), Perl ($N = 9, M = 3.67, SD = 1.25$), and Ruby ($N = 9, M = 3.33, SD = 1.76$).

Participants gave 96 responses to the question, "What soft skills are important to your job?" Answers could be grouped into 14 categories. The most frequently listed soft skill was communication ($N = 21$), and four of the next five most frequently listed skills seemed to be a subset

Table 2. Results of Open-Ended Questions about Soft-Skills

Soft Skill	Importance to Job	
	n	*M* (*SD*)
1. Communication (general)	21	5.43 (0.79)
2. Written communication	13	5.08 (1.07)
3. Public speaking and giving presentations	11	4.64 (1.61)
4. Collaboration collaboration coordinating with people giving and receiving feedback teamwork relationship building	10	5.40 (0.49)
5. Communication with clients and users	10	5.10 (1.22)
6. Communication with upper management	8	5.00 (1.00)
7. Working independently analytical and critical thinking task prioritization time management working under pressure	6	5.50 (0.50)
8. People skills active listening humor tactfulness working with difficult people	5	4.20 (1.47)
9. Management	4	5.00 (0.71)
10. Networking and career management	3	5.33 (0.47)
11. Flexibility learning quickly adaptability	2	5.50 (0.05)
12. Confidence	1	6.00 (n/a)
13. Meetings	1	5.00 (n/a)
14. Note-taking skills	1	5.00 (n/a)

Soft skills reported in order of most to least frequent responses. Similar responses have been combined to form a category. Category names are numbered, and any other responses grouped into that category are listed beneath the category name. Listed under the Importance to Job column are number of respondents (*n*), mean importance rating (*M*), and standard deviation (*SD*).

of communication: written communication, public speaking, communication with clients, and communication with management (Table 2). The fourth most frequently listed skill set, collaboration ($N = 10$), also relies heavily on communication skills. Participants indicated that communication skills were necessary for high job performance because many critical tasks involved close coordination with coworkers (such as when attacking or defending). Many also pointed out that communicating one's technical knowledge in a non-technical way was crucial to maintaining a job in cybersecurity. "You can't be a pen tester if you can't tell people what you did and why it's important," explained one participant, and many others echoed the sentiment that successful cyber professionals are able to explain their job to clients and management and to justify the costs incurred. Technical writing skills as well as general communication skills were characterized as important for getting promoted and transitioning to management positions.

In response to the other open-ended questions, participants mentioned additional KSAs that were important to their job. There were many unique answers, but the skills and abilities most often mentioned by participants included persistence and the ability to stay self-motivated, curiosity and interest in the job, keeping up with changes in technology and methodology, researching skills (in particular, "knowing how to Google"), and knowledge of logic.

When asked which KSAs that had been covered in the multiple choice and open-ended questions were most important to their job, participants gave 60 responses. Eighteen (30%) of responses referred to soft skills, communication skills in particular. Other KSAs mentioned multiple times pertained to vulnerability assessments, networks, programming, adaptability, and keeping up with changes in technology and methodology.

3.2 Where Do Cybersecurity Professionals Learn These KSAs?

For 31 of the 32 NICE KSAs, participants learned the most about the KSA from their job (Table1); on average, 56.02% of participants responded that they had learned the most about any given KSA at work. The exception was "Programing language structures and logic" (KSA #12), which 45% of respondents learned mostly at school. In order, the participants learned the most about the NICE KSAs through their job, self-study (16.27% of responses), school (11.29%), and then other (6.09%). An average of 10.33% of respondents had not learned each KSA.

The intention behind asking participants where they had learned a NICE KSA was that if few participants had learned a KSA in school then that would suggest that existing cybersecurity curricula do not adequately cover the KSA. However, as we will expand upon in the discussion section, the diversity of our participants' educational experiences indicates that our data do not provide information about current curricula and whether it meets the demands of the cybersecurity workforce. Instead, this question provided a second means of measuring a KSA's importance. A lower number of respondents who had not learned a KSA (listed under the "n/a" column in Table 1) conceivably indicates that the KSA should be prioritized more highly when designing course curricula. The percentage of respondents who had not learned a KSA had a strong negative correlation to the KSA's mean importance rating ($r = -0.83$, $p < 0.001$). Three KSAs (Nos. 4, 6, and 13) were learned by all respondents.

When asked where they had learned the soft skills that were important for their jobs, participants were divided. About half indicated that communication skills are innate or strongly dependent upon personal characteristics. "Most [of these skills] are who you are, not things you can learn," said one participant. Other respondents said that they had learned these skills through school or on the job. Skills learned on the job were often those that required dealing with others in an unequal power dynamic, such as when "translating [security jargon] to management" or "[being] sure not to point fingers" at a client experiencing a security breach.

3.3 What Tools Do Cybersecurity Professionals Use?

Participants were asked which tools they used for seven cybersecurity tasks and could give multiple responses (Table 3). The most popular tools overall were Wireshark (66 responses), Nmap (34), and tcpdump (21). The most common responses when asked about recovery and intrusion detection were that the participant used no tools for these tasks. This may be due to the low number of participants with incident response jobs.

3.4 What Do Cybersecurity Professionals Wish They Had Learned in School?

Participants were asked, "Was there anything you've had to learn on the job that you wish you had learned in school?" Of the 57 responses, soft-skills were mentioned most frequently (13 times). In particular, participants had wished they had received instruction on knowledge and skills related to

Table 3. Cybersecurity Tools

Cybersecurity task	Tool	*n*
Recovery	none	15
	custom/proprietary	5
	Window's backup	4
Scanning or port scanning	Nmap	24
	Nessus	5
	custom/proprietary	4
	none	4
	tenable	3
	Rapid7	3
Intrusion detection	none	11
	Snort	10
	custom/proprietary	9
	McAfee suite	3
	Panorama (Palo Alto)	3
Network traffic analysis	Wireshark	25
	tcpdump	9
	none	5
	custom/proprietary	3
	network flows (Linux)	3
	pcap (Linux)	3
Packet-level analysis	Wireshark	24
	none	11
	tcpdump	5
Penetration testing	MetaSploit	14
	Kali Linux	12
	custom/proprietary	7
	none	7
	Burp Suite	5
	Nessus	4
Network analysis	Wireshark	14
	none	10
	custom/proprietary	6
	Nmap	6
	tcpdump	5

Responses mentioned more than twice are reported. *n* refers to the number of respondents who mentioned they used that tool (or no tool) to accomplish the cybersecurity task.

business and office politics (e.g., how to effectively talk to management). Other responses included KSAs related to networking (mentioned six times), programming (six), electrical engineering (two), operating systems (two), packet analysis (two), reverse engineering (two), and specific tools (Burp Suite and PowerShell).

Some participants also provided insight into what they look for in prospective hires who have recently graduated from college. Again, communication skills were emphasized. "I have fired smart students who couldn't understand what management was trying to say," said one participant.

Others talked about the struggle of teaching new hires how to write good tech reports especially when, as one participant put it, "the client is paying $2,000 for a piece of paper."

A few participants thought it was important for undergraduates interested in cyber to gain strong computer science fundamentals and understanding of security methodologies. They characterized this knowledge as being consistent across time whereas the other KSAs were characterized as changing so often that a successful cyber personnel must stay relevant through constant research and self-study.

4 DISCUSSION

Our study was designed to aid the educators implementing the NICE framework's KSAs into their cybersecurity curriculum. We addressed two limitations of the framework: (i) that it does not indicate the relative importance of each KSA and (ii) that it does not indicate whether existing educational programs already adequately meet the needs of the cybersecurity workforce. In addition, we collected information outside of the purview of the NICE framework that might be beneficial to cyber educators. This information included tools used to perform some cybersecurity tasks, programing languages/scripts, and soft skills relevant to cyber work.

Data were collected anonymously at two premier hacker conferences within the United States. Forty-four conference attendees participated, more than participated in other studies that collected in-person data from cyber professionals [22–25]. We are reasonably confident that our participants represent a diverse sample of the US cyber attacking and defending workforce. Participant experience levels, education, and specialty area were varied. Twenty percent of respondents did not have a college degree, which is consistent with the level of previous surveys [26]. Based on the participants who disclosed some information about their employer, participants worked for a variety of companies and government agencies and thus represent a rich collection of experiences within the cybersecurity field.

All 32 KSAs from the NICE framework that were included in the interview were rated as being of above neutral importance (above 3.5 on a 6-point scale). This confirmed our assumption that the 32 KSAs that were listed under multiple specialty areas would be most important to professionals who worked in the protect and defend knowledge area. Furthermore, 15 of these KSAs were found to be significantly more important than neutral after a series of one-sample *t*-tests. This suggests that these 15 KSAs should be prioritized when building course curricula. Within the 15 most important KSAs, educators could prioritize what is covered in their curriculum based on mean importance ratings, how widespread is the knowledge of that KSA, or a combination of those two factors.

The results from the *t*-tests and from the open-ended questions indicate that KSAs related to networks, vulnerabilities, programming, and communication are the most important for cybersecurity students to know upon graduation. Of the 15 NICE KSAs that were significantly more important than neutral, 8 dealt with networks (KSA Nos. 1, 2, 4, 5, 10, 11, 14, and 15), 6 dealt with threats (including vulnerabilities and attacks; KSA Nos. 3, 6, 7, 8, 9, and 14), and one dealt with programming (KSA No. 12). Communication was by far the most important soft skill that cyber professionals found important for their job. When asked about the KSAs that were most important to their job overall, communication, vulnerability assessments, networks, and programming were mentioned multiple times. In addition, communication, networking, and programming were the most frequent responses to the question, "Was there anything you've head to learn on the job that you wish you had learned in school?"

We found that most KSAs were learned primarily on the job or through self-study. This confirms previous perceptions [8]. The exception was the KSA "Programing language structures and logic," which was primarily learned at school. Unfortunately, due to the way that our question was worded and due to the diversity of our participants, it is impossible to conclude whether the other KSAs

are being adequately addressed in course curricula. It is possible that most participants learned about each KSA at school but then gained a deeper comprehension of them later; because we asked where our participants had learned the *most* about each KSA, we were unable to capture these kind of data. Additionally, our participants ranged widely in experience levels and education levels. It is likely that some participants attended college too early to have learned about these KSAs in school. Nearly a fourth of our sample did not complete a post-secondary degree, and a fifth received degrees that were not related to computer science. Therefore, the data we collected on this topic do not provide a good indication of whether a KSA is adequately covered in current cybersecurity programs.

The data presented here provide a means to assess which topics should be included in a course, but further research should be done to determine how best to implement these KSAs in the classroom. Some prior research investigates the ways in which cyber and information science is most effectively taught [27–29] and how to evaluate classroom learning [12]. Ideally, such education research should be done on the NICE KSAs, particularly those rated as being the most important by industry professionals.

The data are most helpful for curricula that intend to focus on the KSAs present in the NICE framework and to provide a general education of the protect and defend knowledge area. Our findings indicate additional KSAs not included in the cyber framework that could be included in curricula. In particular, communication skills and knowledge of Python are important to cybersecurity professionals [23, 25]. Follow-up research could be conducted to verify the findings of the open-ended answers in this study. Future research could also investigate the more specialized KSAs from the four specialty areas within the protect and defend knowledge area so that educators may create more specialized curricula.

ACKNOWLEDGMENTS

The authors would like to thank Dennis Harris for his data collection efforts and Alexandra Krenek for her assistance in organizing and formatting the data.

REFERENCES

[1] Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel. 2004. *The Economic Impact of Cyber-Attacks.* Congressional Research Service Documents, CRS RL32331, Washington, D.C.

[2] Center for Strategic and International Studies. 2016. Hacking the skills shortage: A study of the international shortage in cybersecurity skills. Center for Strategic and International Studies, Washington, D.C. Retrieved April 12, 2017 from https://www.mcafee.com/fr/resources/reports/rp-hacking-skills-shortage.pdf.

[3] Andrew McGettrick. 2013. Toward curricular guidelines for cybersecurity: Report of a workshop on cybersecurity education and training. Retrieved September 19, 2017 from https://pdfs.semanticscholar.org/a420/4367370eda2f4d79fba62693fbe67b71317a.pdf.

[4] Dan Restuccia. 2015. Job market intelligence: Cybersecurity jobs. In *Burning Glass Technologies.* Retrieved September 19, 2017 from http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf.

[5] Alex Vieane, Gregory Funke, Robert Gutzwiller, Vincent Mancuso, Ben Sawyer, and Christopher Wickens. 2016. Addressing human factors gaps in cyber defense. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 60.* Sage GA: Los Angeles, CA, 770–773.

[6] Dan Shoemaker, Anne Kohnke, and Ken Sigler. 2016. A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0). Taylor & Francis, Boca Raton, FL.

[7] NICCS. 2017. National initiative for cybersecurity careers and studies: Cybersecurity workforce framework. Retrieved September 19, 2017 from https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

[8] Homeland Security Advisory Council. 2012. *CyberSkills Task Force Report.* U.S. Department of Homeland Security. Retrieved September 19, 2017 from https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf.

[9] Wm. Arthur Conklin, Raymond E. Cline, and Tiffany Roosa. 2014. Re-engineering cybersecurity education in the US: An analysis of the critical factors. In *Proceedings of the 2014 47th Hawaii International Conference on System Sciences (HICSS'14).* IEEE: 2006–2014.

[10] National Security Administration. 2016. Centers of academic excellence in cybersecurity. Retrieved August 8, 2017 from https://www.nsa.gov/resources/educators/centers-academic-excellence/.
[11] Paul Y. Cao and Iyad A. Ajwa. 2016. Enhancing computational science curriculum at liberal arts institutions: A case study in the context of cybersecurity. *Procedia Computer Science* 80, 1940–1946.
[12] Frank H. Katz. 2012. The creation of a minor in cyber security: The sequel. In *Proceedings of the 2012 Information Security Curriculum Development Conference*. ACM: 75–81.
[13] Michael E. Locasto and Sara Sinclair. 2009. An experience report on undergraduate cyber-security education and outreach. In *Proceedings of the Annual Conference on Education in Information Security (ACEIS'09)*. ACM: Ames, IA.
[14] Frank H. Katz. 2005. The effect of a university information security survey on instruction methods in information security. In *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development*, ACM: Kennesaw, GA, 43–48.
[15] Wayne Patterson, Cynthia Winston, and Lorraine Fleming. 2016. Behavioral cybersecurity: Human factors in the cybersecurity curriculum. In *Advances in Human Factors in Cybersecurity*, Springer, Cham, 253–266.
[16] Fred B. Schneider. 2013. Cybersecurity education in universities. *IEEE Security & Privacy 11*, 3–4.
[17] Seymour E. Goodman. 2014. Building the nation's cyber security workforce: Contributions from the CAE colleges and universities. *ACM Transactions on Management Information Systems* 5, 1–9.
[18] Svetlana Peltsverger. 2015. A survey of University System of Georgia cyber security programs. In *Proceedings of the 2015 Information Security Curriculum Development Conference*. ACM.
[19] Miriam E. Armstrong, Keith S. Jones, and Akbar Siami Namin. 2017. Framework for developing a brief interview to understand cyber defense work: An experience report. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 61. Sage CA: Los Angeles, CA, 1318–1322.
[20] DEF CON. Frequently Asked Questions about DEF CON: How much is admission DEF CON, and do you take credit cards? Retrieved September 19, 2017 from https://www.defcon.org/html/links/dc-faq/dc-faq.html.
[21] Alan C. Boneau. 1960. The effects of violations of assumptions underlying the t test. *Psychological Bulletin* 57, 49.
[22] Michael A. Champion, Prashanth Rajivan, Nancy J. Cooke, and Shree Jariwala. 2012. Team-based cyber defense analysis. In *Cognitive Methods in Situation Awareness and Decision Support (CogSIMA'12)*. IEEE, 218–221.
[23] Jennifer Cowley. 2014. *Job Analysis Results for Malicious-Code Reverse Engineers: A Case Study*. No. CMU/SEI-2014-TR-002. Carnegie-Mellon University Software Engineering Institute, Pittsburgh, PA.
[24] Anita D'Amico and Kirsten Whitley. 2008. The real work of computer network defense analysts. In *Proceedings of the Workshop on Visualization for Computer Security (VizSEC'07)*. 19–37.
[25] John R. Goodall, Wayne G. Lutters, and Anita Komlodi. 2009. Developing expertise for network intrusion detection. *Information Technology & People* 22, 92–108.
[26] SANS Institute. 2014. Cybersecurity professional trends: A SANS survey. Retrieved September 18, 2017 from https://www.sans.org/reading-room/whitepapers/analyst/cybersecurity-professional-trends-survey-34615.
[27] Art Conklin. 2006. Cyber defense competitions and information security education: An active learning solution for a capstone course. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*. IEEE: 2006.
[28] Martin Mink and Felix C. Freiling. 2006. Is attack better than defense? Teaching information security the right way. In *Proceedings of the 3rd annual conference on Information Security Curriculum Development*. ACM: Kennesaw, GA, 2006.
[29] Rose Shumba. 2004. Towards a more effective way of teaching a cybersecurity basics course. *ACM SIGCSE Bulletin* 36, 108–111.

Received April 2017; revised September 2017; accepted October 2017