Exploring the Value of Non-Technical Knowledge, Skills, and Abilities (KSAs) to Cybersecurity Hiring Managers

Lori L. Sussman
University of Southern Maine

Industry's demand for cybersecurity workers with non-technical knowledge, skills, and abilities (KSAs) that complement technical prowess is not new. The purpose of this study was to connect with cybersecurity practitioners to determine which non-technical KSAs should be emphasized by educators to help meet workforce demands. This research applies a novel application of the Ground Truth Expertise Development Model (GTEDM) for exploring suitable non-technical and particularly soft KSAs necessary for cybersecurity professional development programs. This study focused on the definition and competency determination step and provided foundational KSA prioritization for further research. The field overwhelmingly agreed that non-technical skills were essential to a cybersecurity worker's success. The qualitative process produced three themes as non-technical KSA areas of the most significant import to the cybersecurity field. These KSA themes required included critically using information, communications skills, and collaboration to pursue customer/client success. The findings produce a more comprehensive list of hard, soft, and mixed non-technical skills that will benefit the public, private, and academic sector organizations as they develop cybersecurity curricula.

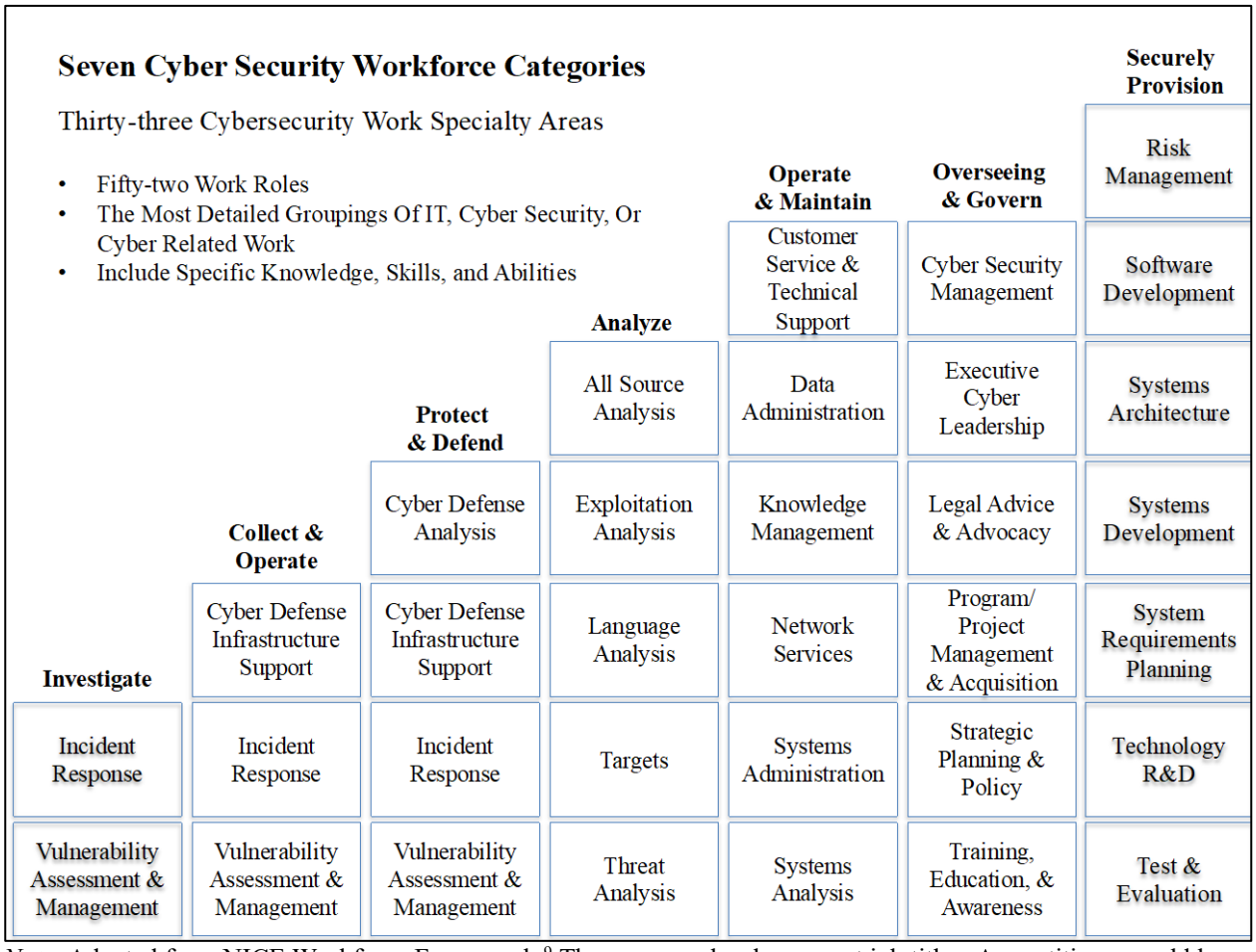
Keywords: cybersecurity skills, cybersecurity education, cybersecurity curriculum, KSA, non-technical skills, cybersecurity training, cybersecurity roles

INTRODUCTION

Cybersecurity leaders have taken aggressive actions to hire people with the right expertise over the past ten years yet remain understaffed.[1-4] Even before the COVID-19 pandemic created a massive pivot to remote working, reports of cyberattacks, social engineering scams, identify theft, and cyber-based financial fraud frequently made news headlines.[5-6] The pandemic simply exacerbated the existing cybersecurity staffing problems as significant numbers of workers went remote and needed secure connected technology to work at home.[7] The research indicates increased difficulty hiring cybersecurity professionals with requisite skills and expertise through 2030.[2]

NIST responded to this need for more cyber professionals through its National Initiative for Cybersecurity Education (NICE) organization. NICE brings industry, government, academia, and non-profit organizations together to address the U.S. cybersecurity education, training, and workforce needs.[1] NICE uses the expertise model that contains three interrelated components of knowledge, skill, and abilities to formulate cybersecurity work roles to create a shared picture of today's cybersecurity worker (see Figure 1).[8-9]

FIGURE 1
NICE CYBERSECURITY WORKFORCE FRAMEWORK



Note. Adapted from NICE Workforce Framework.[9] These are work roles are not job titles. A practitioner could have one or more work roles assigned to their position.

However, one delving into the NICE Workforce Framework, it is readily apparent that there are extensive technical KSA specifications but little guidance as to requisite non-technical ones.

Expertise Requires an Expression of Skill

Two systems commonly represent expertise. One system is factual (technical), and the other heuristic (non-technical) KSAs.[10] The cybersecurity field often equates non-technical KSAs with the term "soft skill." The cybersecurity field considers non-technical KSAs like problem-solving, communications, collaboration, and similar behaviors to be soft skills.[11-12] It is important to note that not all non-technical skills are soft, but soft skills are often of most significant interest to employers when hiring.[12]

The inclusion requirement for non-technical skills, and particularly soft skills, into cybersecurity worker development is not new. The literature showed non-technical secondary traits enhance the expression of expertise.[14] The survey of 315 security professionals from over 100 US-based companies about cybersecurity skills gaps by Tripwire illustrates this point. The respondents noted that soft skills were essential for cyber worker success.[2] Study findings showed that the need for soft skills had increased to the point where employers were willing to hire people with strong soft skills even if they had not technical cybersecurity expertise.[2] In their 2020 survey update, Tripwire noted company security teams were highly strained due to difficulty staffing and continued to look for external assistance to address the skills gap.[3]

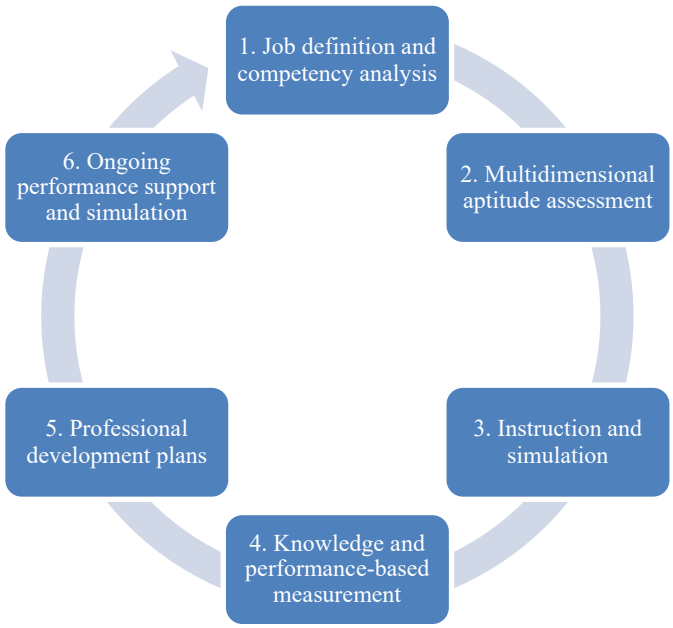
Tripwire's data underscore the need to integrate technical and non-technical KSAs into curricula for every cybersecurity role. The purpose of this study was to connect with cybersecurity practitioners to explore which are the most critical non-technical KSAs to teach in future workers.

Developing a Conceptual Framework

Hiring managers identify the multidisciplinary KSAs that fall under the Association of American Colleges and Universities VALUE rubrics as necessary KSAs for technical workers to get hired.[13] There appears to be a two-stage recruiting model where requisite technical skills get candidates past the filters to an interview. It is the interview step that is most crucial in the hiring process. Hiring managers assessed candidates for their demonstrated soft skills and cultural fit as top hiring criteria.[12] Research found that hiring officials looked for inquiry and analysis, critical thinking, creative thinking, written communication, oral communication, reading, quantitative literacy, information literacy, teamwork, and problem-solving KSAs in future workers.[12-13] This study used non-technical KSAs gleaned from the current NICE Cybersecurity Framework as a starting point to discuss with cybersecurity professionals. The subsequent qualitative analysis used categories noted by AACU for categorization and analysis. Contemporary theory informed the qualitative process used when exploring the significance of non-technical KSAs with cybersecurity practitioners.

The present Cybersecurity Workforce Framework had some non-technical KSAs, and the researcher mapped them to the GTEDM model, thus producing a conceptual framework for analysis. A conceptual framework uses theory, research, and experience to examine the relationship between constructs and ideas.[15] In this case, the Ground Truth Expertise Development Model (GTEDM) and its first step requiring job definition and competency analysis provided an effective way to look at those KSAs that fall under the baseline non-technical skills examined.[16] GTEDM's six significant areas are understand, assess, educate, measure, develop, and get feedback to create cybersecurity experts who will help continually improve the field.[16] The GTEDM provides the path to expertise that educators can use to map student progress developing necessary non-technical KSAs (see Figure 2).

FIGURE 2
THE GROUND TRUTH EXPERTISE DEVELOPMENT MODEL (GTEDM)



Note. Adapted from Assante and Tobey, this model helps identify and develop future cybersecurity experts.[16]

As noted by the National Board of Information Security Examiners (NBISE) (2012), non-technical skills help differentiate experts from those who were competent (journeyman) or proficient (apprentice).[17] The NBISE concluded that identifying technical and non-technical cybersecurity KSAs at each point in a professional's progress from apprentice to journeyman could allow educators to develop curricula that engender accelerated development.[17]

To get clear definitions for the GTEDM, the investigator engaged field experts to share their views on essential non-technical KSAs currently missing. Since defining KSAs are part of the "Understand" phase of the GTEDM, the investigator bound much of the conversation with the participants to the early career stage. Some interviews touched upon subsequent steps of the GTEDM, but that was relatively limited. The use of published KSAs from the current NICE Cybersecurity Workforce model served to get immediate participant acceptance of the KSAs presented for their review. The cybersecurity field experts' involvement and insights produced rich data necessary for job definition and competency analysis.[16] As such, this conceptual model helped bound the inquiry process and provided ideas for future investigation.

The investigator interviewed 43 self-identified cybersecurity professionals from industry, non-profits, government, and higher education. This study focused on exploring non-technical KSAs that experts believed were instrumental to a cybersecurity worker's success. This work focused on answering two research questions concerning the relative importance of the non-technical KSA gaps. The first question addressed the degree of importance cybersecurity professionals placed on non-technical KSAs for their entry-level and other cybersecurity workers. The second question centered on soliciting opinions about the most urgent, if any, non-technical KSAs that the future NICE Cybersecurity Workforce Framework should consider adopting. (see Table 1).

TABLE 1
TECHNICAL CYBERSECURITY ROLE NON-TECHNICAL KSAS

Competencies	**Non-technical KSAs**
Hard	• Knowledge of and compliance with legal and regulatory • Managing crisis situations, such as fires, employee or guest injuries, tornados, etc. • Using computers effectively
Soft	• Customer service problem resolution • Developing positive customer relations • Facilitating teams and teamwork • Leadership abilities • Managing personal stress • Negotiating techniques • Presentation skills • Professional demeanor and appearance • Using ethics in decision making • Working effectively with peers • Written communication skills
Mixed	• Critically using information for decision making • Training employees

Note. Adapted from Sisson and Adams[23]

The study design used a grounded approach for data collection and interpretation of KSAs discussed and recommended by the participants. This method allowed the researcher to create appropriate non-technical KSA recommendations for technical cybersecurity professionals based on theoretical models discussed.[13, 18, 19]

Methods

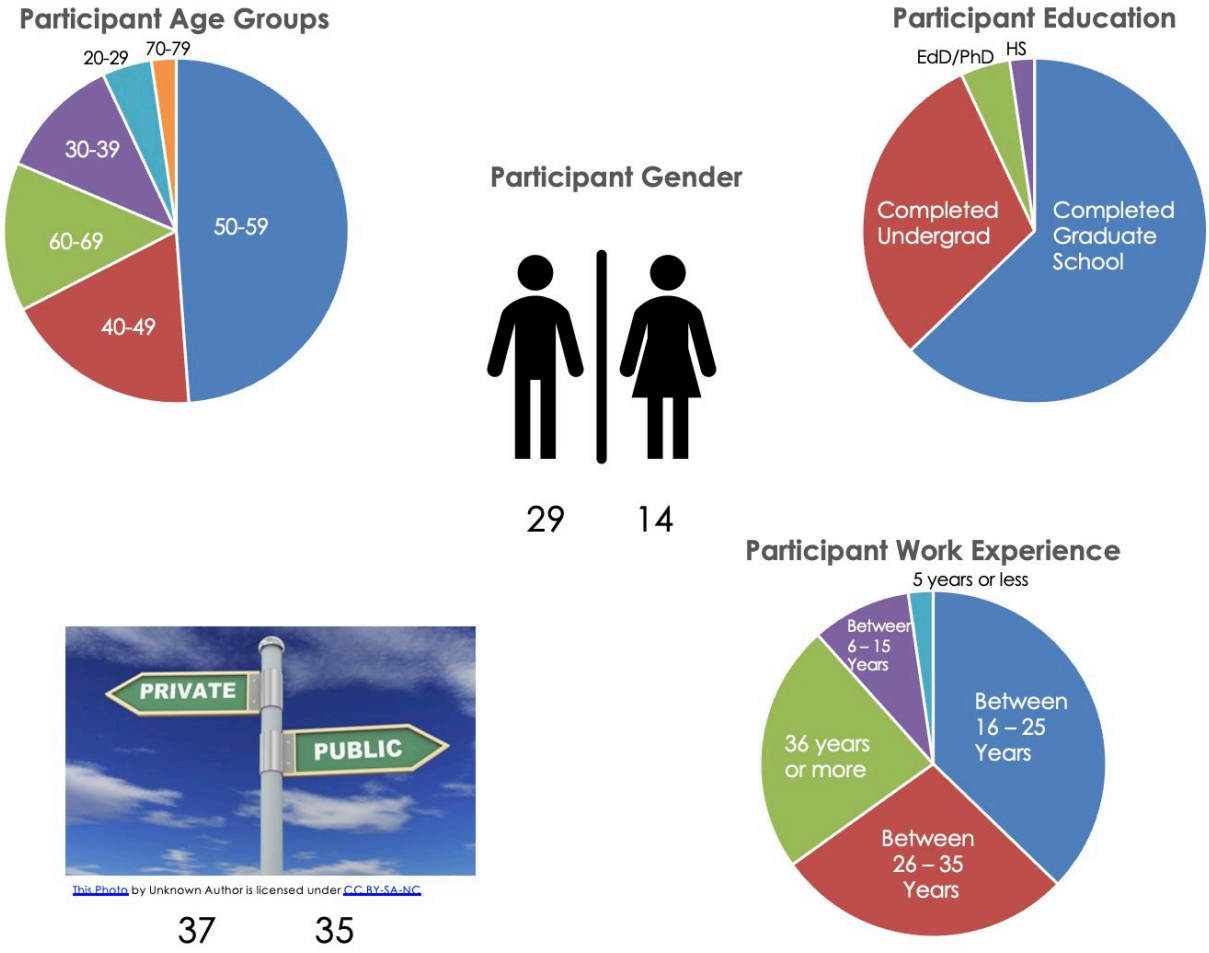
The investigator used a phenomenological study method using both structured and semi-structured methods for collecting data. For three months, the investigator conducted semi-structured interviews with cybersecurity professionals who performed a wide variety of cybersecurity roles. The participants received an advance copy of KSAs listed in Table 1 for review before the scheduled session. Interviews provide a richness of data and the latitude to ask follow-up questions. This ability to pursue detail puts the researcher in a unique position to probe and clarify, thus using the interview as a mechanism to encourage participants to add other pertinent information.[20]

Social media such as LinkedIn provided an effective mechanism to request participation from self-described cybersecurity professionals. There were over 100 initial responses, 65 initial intakes, 45 interviews, and 43 returned approved transcripts. Participants agreed to Zoom recordings of their talks, which accelerated transcription with its automated cloud transcription capability for enterprise users. The principal investigator reviewed and corrected the automatic transcription before sending the document to the participants for review and approval. The transcripts were stored without personal identifiers and uploaded into NVIVO for qualitative coding. The researcher did not compensate participants for their involvement with this study.

Purposeful Sampling

The investigator narrowed the sample population to those who explicitly used cybersecurity as part of their job description or title for this study. As a grounded theory study, the researcher found that these cybersecurity professionals provide the most authoritative reasoning behind non-technical skills essential for new worker professional development.[20] The 43 interviews represent a wide range of roles, from cybersecurity executives at a Fortune 50 company to individual contributors working in small businesses. This use of maximum variation sampling provided substantial variation in perspectives, experiences, and exposures, thus offering greater insight into the phenomena that shape the need for non-technical KSAs.[20] The researcher was open to snowballing, and several participants identified others for this study. The NICE Workforce Framework provided the definitional boundary for cybersecurity professionals and guided recruitment. The resulting pool was more diverse and senior than the cybersecurity field writ large (see Figure 3). According to ISC(2),[21] the workforce is over 66% male, 38% completing a bachelor's degree, 28% achieving a master's degree, and 10% doctoral or post-doctoral degrees. The workforce is also relatively young, with 37% under 35 years of age, 33% between 35 and 44, 19% between 45 and 54, and less than ten over 55.

FIGURE 3
PARTICIPANT DEMOGRAPHICS



This participant sample was 67% male. The group was also more educated, with 29% having a bachelor's degree, 64% completed a master's degree, and 5% had a doctorate or higher. The group was a bit older than the field, with 66% being 50 or older, 17% in their 40's, 12% in their 30's, and 5% in their 20's. These minor variations from the field demographics helped get the hiring manager's perspective during the interviews.

Data Collection

The data collection phase consisted of 43 semi-structured interviews planned for 45 minutes and did not exceed one hour. The interview questions used non-technical KSAs derived from the current NICE Workforce Framework. The investigator asked each participant about the relative importance of these KSAs for more technical cybersecurity workers. The interviewer then asked them to identify what was missing from the list provided. Knowledge, skills, and abilities were all discussed separately.

The first three interviews served as a pilot to discern potential flaws and timing challenges. Because there were no revisions to the protocol, the researcher included data from these interviews in the final data set. This approach aligns with accepted qualitative research methods. The researcher coded the data until reaching theoretical saturation, the point at which no new themes or ideas emerged from the data.[20]

Analysis

Data collection is a series of interrelated activities that include locating the individual, gaining access and making rapport, purposeful sampling, collecting data, recording the information, resolving field issues, and storing data.[20] This study followed these steps at the macro level for its methodology. Moustakas (1994)[22] suggests that a phenomenological interview be informal, interactive and uses open-ended comments and questions to get the participant to share their whole story. Also, this study used this philosophy for instrument construction. These frameworks provided valuable synergies to reach an optimal research methodology.

Data analysis involved a detailed coding process, pattern-matching, and meaning-making.[20] The researcher used software tools to remain objective and rigorous in the investigation.[20] One requires this kind of strategy to successfully use this type of software, including putting information into thematic arrays, creating a matrix of contrasting categories and placing evidence underneath, creating visual displays, tabulating the frequency of different events, and creating chronological or other types of sequence.[20] Using Computer-Assisted Qualitative Data Analysis Software (CAQDAS), the researcher first coded to develop meaning units. Subsequent coding iterations collapsed categories, clustered KSAs into common categories, and created textural descriptions of the participants' experiences.[20, 23]

The non-technical skills fell into three major nodal categories of hard non-technical KSA, soft non-technical KSA, and mixed non-technical KSAs.[23] The hard non-technical KSAs included knowledge of core business processes, using computers effectively, knowledge of and compliance with legal and regulatory requirements, and managing crises. Not surprisingly, the list of soft skills was the most extensive (see Table 2).

TABLE 2
SOFT SKILLS CODED

Nodes	Skills
Soft competencies	Presentation skills
Soft competencies	Developing positive customer relations
Soft competencies	Customer Service Problem Resolution
Soft competencies	Written communications skills
Soft competencies	Working effectively with peers
Soft competencies	Facilitating teams and teamwork
Soft competencies	Intellectual curiosity
Soft competencies	Adaptability
Soft competencies	Professional demeanor
Soft competencies	Negotiating techniques
Soft competencies	Ethics in decision making
Soft competencies	Managing personal stress
Soft competencies	Leadership abilities

The mixed non-technical KSA was the shortest list that included critically using information for decision making and training. Data saturation occurred by the thirty-third coding, but the researcher continued to code all participant data to achieve trend data for KSA recommendations. Coding all participant data produced qualitative themes based on category aggregation and trend data based on nodal references.

The researcher used pattern coding to group summaries into smaller numbers of categories.[20] These pattern codes identified both emergent themes and explanatory groupings. The pattern coding led the researcher to construct the assertion that non-technical KSAs were significant to a cybersecurity worker's professional success and development. Clustering under the NICE Cybersecurity Framework KSAs developed over the second and third coding cycles. The CAQDAS tool supported a super coding analytical process where relationships between codes enabled future reflection and continued analysis.[20] The pattern

codes collapsed into NICE Cybersecurity Framework KSAs that provide insight into the participant's emphasis on some aspects of the baseline KSAs presented during the interviews. The resulting themes and inferences from coding clusters helped the researcher construct valuable recommendations for non-technical KSAs that educators should include in cybersecurity curricula.

Findings

The research design provided significant data use for cybersecurity curricula development. The first research question explored the importance of the cybersecurity field regarding non-technical KSAs for very technical cybersecurity workers. Each participant verbalized their agreement that most non-technical KSAs presented were essential characteristics to consider when hiring for an entry-level position during their interview sessions. The exception was in the area of training. Participants agreed that some kind of ability to train others was an essential part of a cybersecurity workers' professional development, but it is a skill expected of experts. To this point, one cybersecurity expert shared,

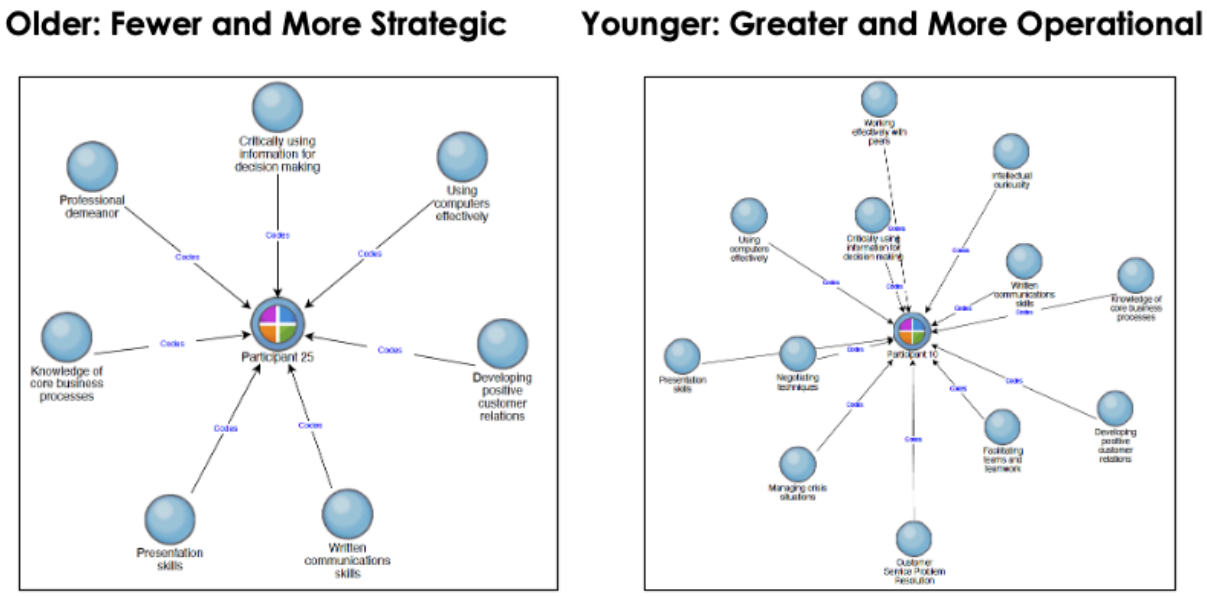
> *Multiple times users will call the security operation center, and the analysts need to walk the user through the resolution of an incident. Many times, it is just simple email phishing. Or spam of some sorts, but the analysts must walk them through remediation, and the analysts have to convey what they are looking at. The user does not know what to do even though they have taken a class on it. Our analysts are now training them step-by-step on what they need to do to remediate that problem.*

In other words, knowledge capture, sharing, and reuse were necessary. Still, the participants did not expect entry-level cybersecurity professionals. Employers expect cybersecurity workers are to develop proficiency training others over time.

There was a range of ideas surrounding which KSAs should rise to the top as the most essential, and some depended on role and experience. The data reflects participant perceptions of proposed non-technical KSAs based on their experience, education, and exposures. This study reinforced the Tripwire findings, where participants unanimously agreed that non-technical skills were indispensable to a cybersecurity worker's success.[2-3]

The second research question probed to find which non-technical skills were the most critical KSAs to address for worker education and training. As the GTDEM indicates, the participants' perceptual lens was heavily influenced their role.[16] A participant's role informed the technical and non-technical KSA conversation to define cybersecurity competency and readiness. The more managerial a participant's position, the more their concern shifted from customer problem resolution to assuring a positive customer experience (see Figure 4). While these disparate points of view did not change the overall list, they did change the emphasis and order of various KSAs.

FIGURE 4
CONTRAST BETWEEN SENIOR VERSUS JUNIOR PARTICIPANTS' NON-TECHNICAL KSAS EMPHASIS



Note. The left diagram represents a participant in an executive role, and the right diagram illustrates a participant in a mid-level operational position.

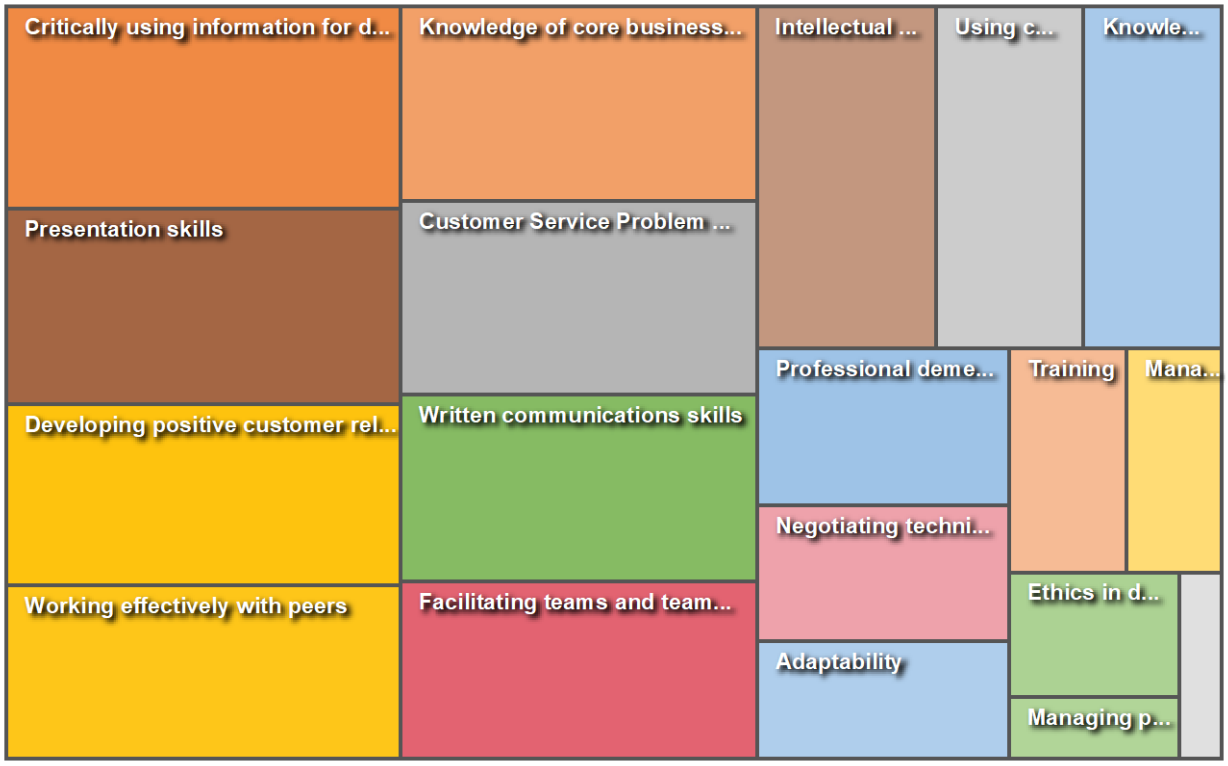
It appeared that this emphasis shift could be due to the difference in strategic versus the operational focus of the participant's cybersecurity role.

One should note that those reviewing this data should refrain from making quantitative inferences from this work. The semi-structured format for interviews provides multiple voices and perceptions. Although the researcher used nodal reference counts to emphasize a particular area, the significance of the trend information did not rely on frequency alone. The weight of insight does not rest solely on the number of participants who voice it. It is instructive to review those areas most often brought up by the participants to harmonize the disparate trend data due to demographic influences (see Figure 5).

FIGURE 5
SUMMARY WORD CLOUD DENOTING PARTICIPANTS' AGGREGATE EMPHASIS AREAS

Parallel to the data collection effort, the researcher performed open coding to label, look for meaning, and categorize the data. The investigator generated a codebook used to evaluate all 42 interviews. By iteratively coding, salient concepts emerged from the interviews. These activities led to the development of a codebook. The author then used this codebook to code the interviews deductively. This process produced three themes as non-technical KSA areas of the most significant import to the cybersecurity field. These themes required included critically using information, communication skills, and collaboration to pursue customer/client success. These clusters aggregated across roles, ages, and education and were reasonably uniform as they were (see Figure 6).

FIGURE 6
AGGREGATED PARTICIPANT RESPONSE HIERARCHY MODEL



It is significant to note that the CAQDAS clustering did not indicate significance based solely on the number of items coded but included the number of participant references to a particular skill. After several code-checking iterations, the skill references breakout showed soft non-technical skills as the most significant area (see Table 3).

TABLE 3
TOTAL CODING ROLL-UP OF ALL NON-TECHNICAL KSAS BY TYPE

Nodes	Skills	Number of coding references	Number of items coded
Soft	Presentation skills	153	40
Soft	Developing positive customer relations	145	38
Mixed	Critically using information for decision making	140	41
Soft	Customer Service Problem Resolution	134	39
Soft	Written communications skills	117	36
Soft	Working effectively with peers	114	37
Hard	Knowledge of core business processes	104	38
Soft	Facilitating teams and teamwork	96	34
Soft	Intellectual curiosity	84	35
Hard	Using computers effectively	64	30
Hard	Knowledge of and compliance with legal and regulatory requirements	63	29
Soft	Adaptability	48	22

Soft	Professional demeanor	46	19
Soft	Negotiating techniques	30	16
Hard	Managing crisis situations	26	13
Mixed	Training	14	10
Soft	Ethics in decision making	14	10
Soft	Managing personal stress	5	4
Soft	Leadership abilities	3	3

The stress on soft skills as essential non-technical KSAs for technical cybersecurity roles is a critical finding supporting the current literature specifying the workforce's desirability of these skills.[3-4]

Critical Thinking Using Intellectual Curiosity and Creative Problem Solving

Participants valued attitude over aptitude for many roles, but especially for entry-level positions. The technical prowess that a cybersecurity worker brings to bear is only helpful if that person can integrate critical thinking, reading, listening, and writing skills to solve the client or customer's problem. As one cybersecurity manager who works at a cybersecurity consulting firm explains,

> *One of the things that I find lacking in many of the individuals who go into cybersecurity, especially junior analysts, is that they do not understand what is being done. For example, on the data loss prevention tool, the alert will fire, and the analyst will look at the alert, and they are translating it from a literal perspective. They do not understand that the software is scanning for number sequences, and that is what triggers the alert. If you understand the concepts of either the application, the software, or the equipment and how it's being applied, then analysts can actually better understand how to go about responding to the information that's provided to them.*

The field sent a clear message that cybersecurity workers need to be intellectually curious. That need to find an answer pushes them to research and better understand the technical and business environment holistically. In this way, these workers use critical thinking skills to elevate their technical knowledge, problem solve and resolve client issues quicker.

The difference in participant experience did impact emphasis. There was a corresponding emphasis on the customer/client experience based on the participant's seniority (see Table 4). KSAs such as training, critical use of information for decision-making, and presentation KSAs rose to the top for more experienced participants.

TABLE 4
PARTICIPANT EMPHASIS BY AGE

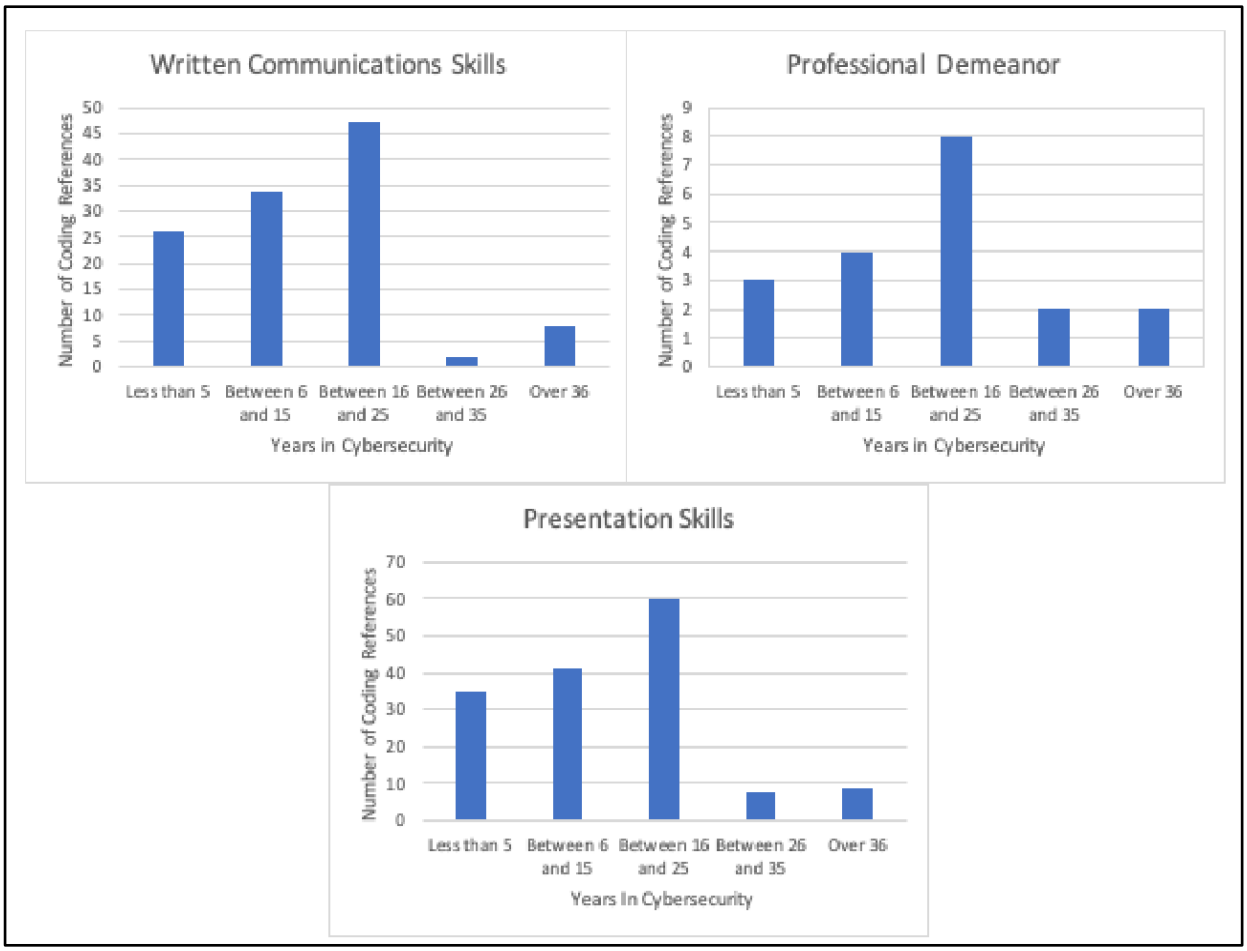
Older Participant Priorities	**Younger Participant Priorities**
Developing Positive Customer Experiences	Working Effectively with Peers
Critically using information for decision	Facilitating Teams and Teamwork
Professional Demeanor	Customer Problem Resolution
Presentation Skills	Intellectual Curiosity
Written Communications Skills	Using Computers Effectively
Knowledge of Core Business	Critically using information for decision
Training	Managing Crisis Situations

In contrast, more operationally focused participants looked for qualities that helped them integrate better into the cybersecurity team to enhance client problem resolution. Despite the differences, all the participants had similar lists, and only the emphasis differed.

All KSAs Are Essential, but Emphasis Varies

As noted by most participants, not all cybersecurity jobs are the same, so the KSAs required for that work differ. An example is the way a worker communicates may vary dependent on the role. As one executive shared, *"we have a lot of people in cyber that people would say, are quiet, introverted, geeky, but everybody has to be able to communicate."* That statement reinforces the reality that cybersecurity is rarely a solo effort, and workers must present information to the team as a minimum capability. As such, oral and written skills are keenly essential to work effectively in cybersecurity roles (see Figure 7).

FIGURE 7
EMPHASIS ON COMMUNICATIONS KSAS BY ALL PARTICIPANTS



Note. Age and position impact priority in the hierarchy of necessary non-technical KSAs.

One participant summed up how difficult but vital it is to have strong communications skills by explaining that,

> *"they may be talking to other technical people that may interact with the businessperson during a one-off conversation. [However,} thinking and then really challenging that other technical person or going directly to the business to get the underlying reasons for these requests, these use cases, and not just purely turning on feature sets or turning on capabilities. Getting deeper in a way that taxes communication skills. I think we don't do justice, even in our hiring process, of identifying those communication skills. This is hard."*

Most participants combined critical thinking with the need for communication skills that keep the team and customer informed. Many spoke of the need for employees to present at the group rather than the customer level. Those under fifty spoke passionately about preserving the diversity of talent by making it acceptable to use various means to communicate with peers. Regardless, the participants uniformly expected any individual contributor to work effectively with peers utilizing some type of oral, written, or visualization tools.

Cybersecurity Workers Must Be Multifaceted Collaborators

As noted in over 90% of the interviews, cybersecurity is part of everything in the increasingly connected world. One participant noted that "*as cybersecurity professionals, one of the hardest things that we have to deal with on a general basis is that cybersecurity is a part of everything. It's not like it is its own thing. You can't just do security without all of the people around you."* Yet, collaboration does not look the same for every cybersecurity role. Collaboration skills are not just for in-person interactions. Cybersecurity workers must use these skills to resolve technical issues, provide security guidance, and address customer concerns in layman's language. This focus on the needs of others helps the team or organization develop positive customer relationships with clients.

More than 80% of the participants expressed the need for teaming. An executive likened cyber to a basketball team sharing that in cyber, it is "*the same type of communication and ability to clearly explain what you need as you're trying to move the ball down the field quickly*." More than half of the participants talked about the importance of working with peers and sharing knowledge. One manager was very clear that the way a cyber new hire can *"stand out is that they're able to improve the processes, improve the team, based on just being there because they came from and showed they think outside the box. When we take someone from outside of the organization and bring them in, you expect there to be change."* More than half of the participants spoke to how facilitating the team, and team building, ultimately resolved customer issues and fostered client relationships. While collaboration types can be diverse, the participants uniformly agreed that cybersecurity workers must get along with their team and support efforts to create positive relationships with customers.

Recommendations for the Education and Training Curricula

Pattern coding provided instructive inference clustering information that permitted searches for KSA relationships using Boolean search terms of AND and OR with semantic operators.20 This approach produced clustering around the connections between hard, soft, and mixed KSA allowed the researcher to infer emphasis trends. The resulting inferences from coding cluster constructs help develop specific education and training objectives.

The researcher presented the participants with the knowledge elements first. There was disagreement about what was most important at various stages of a cybersecurity professional's career, but the participants deemed all necessary. The knowledge of an organization and core mission areas was the most remarkable clustering area (see Table 5). However, knowledge of communications and computer tools was considered crucial and often referred to as *"a 'table stakes requirement to even get an interview."*

TABLE 5
KSA REFERENCE CLUSTERING AROUND NICE NON-TECHNICAL KNOWLEDGE ELEMENTS

NICE Cybersecurity Workforce Framework Element	KSA references
K0146: Knowledge of the organization's core business/mission processes	987
K0239: Knowledge of media production, communication, and dissemination techniques and method	382
K0246: Knowledge of relevant concepts, procedures, software, equipment, and technology applications	322
K0243: Knowledge of organizational training and education policies, processes, and procedures	266
K0287: Knowledge of an organization's information classification program and procedures for information compromise	155
K0245: Knowledge of principles and processes for conducting training and education needs assessment	108

Participants gave areas such as training less credence since the discussion focused on entry-level workers. However, many participants expected that more senior cybersecurity professionals would teach peers and customers/clients. One experienced cybersecurity professional shared,

> *I would say junior people; I need them to execute their own individual training programs. But journeyman mastery level, yeah, they absolutely need to be involved in developing and executing technical training programs and passing on knowledge. I think that a cybersecurity organization can't thrive if experienced people are not passing on their skills. I think that will fail in the private sector and the public sector. There's too much information.*

There were several recommended additions to the knowledge area, but none clustered sufficiently to get included for consideration

The skills areas clustering provided helpful insight. The clustering around the criticality for cybersecurity workers to convey information effectively is noteworthy (see Table 6). Cybersecurity workers' ability to perform knowledge capture, sharing, and reuse activities took considerable portions of the interviews. To this point, one executive remarked that "talking to others, giving information effectively that cannot be emphasized enough."

TABLE 6
KSA REFERENCE CLUSTERING AROUND NICE NON-TECHNICAL SKILLS ELEMENTS

NICE Cybersecurity Workforce Framework Element	KSA references
S0070: Skill in talking to others to convey information effectively	447
S0066: Skill in identifying gaps in technical capabilities	279
S0166: Skill in identifying gaps in technical delivery capabilities	232
S0296: Skill in utilizing feedback to improve processes, products, and services	168
S0064: Skill in developing and executing technical training programs and curricula	84
S0102: Skill in applying technical delivery capabilities	63

The clustering around the identification of gaps often brought in the need to convey information. The participants expressed that once a cybersecurity worker identified a gap, they must quickly and effectively share this information with their team.

Abilities were the final area discussed with the participants. As shown in Table 7, the professionals interviewed spent most of their time discussing problem-solving, critical thinking, and communications, which showed significant clustering.

TABLE 7
KSA REFERENCE CLUSTERING AROUND NICE NON-TECHNICAL ABILITIES ELEMENTS

NICE Cybersecurity Workforce Framework Element	KSA references
A0118: Ability to understand technology, management, and leadership issues related to organization processes and problem-solving	450
A0119: Ability to understand the basic concepts and issues related to cyber and its organizational impact	426
A0013: Ability to communicate complex information, concepts, or ideas	398
A0070: Ability to apply critical reading/thinking skills	273
A0106: Ability to think critically	240
A0105: Ability to tailor technical and planning information to a customer's level of understanding	186
A0018: Ability to prepare and present briefings	148
A0089: Ability to function in a collaborative environment	120
A0112: Ability to monitor advancements to ensure organizational adaptation and compliance	100
A0019: Ability to produce technical documentation	95
A0024: Ability to develop clear directions and instructional materials	38
A0063: Ability to operate different electronic communication systems	38
A0083: Ability to evaluate information	26

The participants considered areas that dealt with technical documentation that created clear directions as items for more senior cybersecurity workers. That area may have been skewed lower by the focus on more entry-level workers. However, one should not interpret the lack of clustering as non-important areas.

Implications

This study's most insightful implication is that higher education and professional development training organizations that educate and train cybersecurity professionals should consider integrating non-technical KSAs into their programs. The participants, without exception, agreed that cybersecurity workers need to grow non-technical knowledge, skills, and abilities. They diverge on the most important and when, but there is universal agreement that cyber workers must do three key activities. These workers must apply critical thinking when using information for decision-making, hone communications skills that support the broader team, and collaborate to resolve customers' resolution problems. As such, these non-technical KSA meta-areas should be core competencies that cybersecurity professionals master over time.

Expertise requires both factual and heuristic knowledge and the inclusion of the non-technical KSAs into the Cybersecurity Workforce Framework serves to provide the latter component, which is currently missing.[10] Non-technical KSAs such as those represented in Tables 6 through 8 are the underpinning basis for good relationships, sound judgments, and critical reasoning.[10] A knowledge area would stay the same at the three levels of apprentice, journeyman, and expert with a scaffolded model, but the skills and abilities would be different. Cybersecurity certification and credentialing institutions may use these additional KSAs for inclusion in their programs. At a minimum, it would provide a capability maturity model that is currently missing and could help education and training organizations assess what is lacking in their current graduates.

Limitations

This research used a qualitative approach, but the trend data indicates that adding a quantitative component for future studies may yield greater fidelity to additions, deletions, and modifications to the current list of non-technical KSAs. The Boolean searches that yielded the quantity of coding references for each KSA were imperfect due to the semi-structured question format. If future research added a quantitative component, it might allow the investigator to narrow questions and develop instruments to analyze answers using statistics.[20] Qualitative interpretation requires a significant number of cross-checks, but researcher bias can still be problematic. However, this technique provides rich data that could help interpret the results from surveys and provide more significant insights. In turn, the addition of some type of quantitative inquiry could substantially reduce bias, whether perceived or actual.

Another limitation was the number of KSAs offered for participant review. This study's semi-structured interview instrument did not have a comprehensive list of non-technical KSAs for participant consideration. The researcher derived the KSAs for the interviews using the 2017 version of the NICE Cybersecurity Workforce Framework as a baseline. As such, the list produced is more of a starting point for inclusion in the next iteration of the NICE Cybersecurity Framework rather than a comprehensive document. These findings can provide directionality for future studies that can use other instruments to capture missing non-technical KSAs needed by apprentice, journeyman, and/or expert cybersecurity workers.

The final limitation to address is participant demographics. This study's participants are older, more educated, and more senior than the field demographics. Future work endeavoring to create a more expansive non-technical KSA list may want to consider developing a participant sample that is more closely representative of the broader cybersecurity field. The field is at an inflection point where roughly one-third of its most junior workers started as cybersecurity professionals, but more than two-thirds are from feeder fields.[24] As the number of folks coming into cybersecurity from other fields shrink and the number of those who studied it from the beginning of their careers grows, the demand for a guild approach may further influence professional development. The investigator will triangulate the data from this study with future research to reduce any bias introduced through skewed demographics.

Conclusion

Industry, government, and academia share the responsibility to produce trained and ready cybersecurity talent for workforce demands. Organizations will screen talent for their technical skills as a foundational expectation, but their hiring decisions will rest heavily on the candidate's demonstrated soft skills and cultural fit.[12] This research validated the current understanding of this phenomenon. Every participant talked about how soft skills enhanced a candidate's technical skills and are essential attributes they seek in new hires. New cybersecurity professionals will need non-technical hard, soft, and mixed skills to progress in public, private, or non-profit organizations. Some of the most desirable traits include the precise use of information to make decisions, communications, and collaboration. These KSAs do not look the same for all roles but are critical components for employability and professional growth.

Cybersecurity experts deemed it imperative that professionals possess non-technical skills that positively impact relationships with customers, peers, and effective decision-making. Participants diverged in the area of emphasis rather than the inclusion of any particular KSA. More senior participants focused on the customer experience with more references to training clients, critically using information for decision-making, and developing positive client relations. The more junior participants spoke more about customer problem resolution, emphasizing teamwork, positive peer relationships, and problem resolution. From a holistic perspective, participants stressed that the most successful cybersecurity workers were intellectually curious people who show that they could think critically. These practitioners also noted that it was acceptable to have different ways to communicate and collaborate with their organizational stakeholders if the means and modalities were effective. The critical insight was that the definition of communications effectiveness was role-dependent. Often, the discussion was how a worker approached problem-solving, communicating, or collaborating rather than the participant questioning the need to perform these critical KSAs.

Cybersecurity is a fast-paced field that is evolving quickly. There is much to learn, but it does not help future workers to emphasize professional development's technical aspects at the expense of also developing critical soft skills. When one looks critically at cyber work roles, it is clear that these future professionals will need many non-technical skills to help them be advocates for cyber-related projects and remediation activities.[18] The inclusion of non-technical skills scaffolded over a cybersecurity worker's career may have a significant positive impact on their competence, confidence, and effectiveness over time.

ENDNOTES

1. Petersen R. Cybersecurity Insights: A NIST blog: NICE! 10 Years in the making [Internet]. Gaithersburg, MD: National Institute for Standards and Technology; 2019, Nov 12. Available from https://www.nist.gov/blogs/cybersecurity-insights/nice-10-years-making#:~:text=While%20the%20inception%20of%20NICE,held%20until%20two%20years%20later
2. Lapena R. Survey says: Soft skills highly valued by security team [Internet]. Portland, OR: Tripwire; 2017, Oct 17. Available from https://www.tripwire.com/state-of-security/featured/survey-says-soft-skills-highly-valued-security-team/
3. Lapena R. No relief for cybersecurity teams in sight, reveals Tripwire's latest skills gap report [Internet]. Portland, OR: Tripwire; 2020, February 10. Available from https://www.tripwire.com/state-of-security/featured/tripwires-skills-gap-report/
4. Crumpler W, Lewis JA. The cybersecurity workforce gap [Internet]. Washington, DC: Center for Strategic & International Studies (CSIS); 2019, Jan 29. Available from https://www.csis.org/analysis/cybersecurity-workforce-gap
5. Federal Bureau of Investigation (FBI). News. COVID-19 fraud: Law enforcement's response to those exploiting the pandemic [Internet]. Washington, DC: United States Department of Justice; 2020, Jun 9. Available from https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic
6. U.S. Secret Service (USSS). Secret Service issues COVID-19. COVID-19 phishing alert, [Press Release]. Washington, DC: U.S. Department of Treasury; 2020, Mar 9. Available from https://www.secretservice.gov/data/press/releases/2020/20-MAR/Secret_Service_COVID-19_Phishing_Alert.pdf
7. U.S. Bureau of Labor Statistics (BLS). News Release. The employment situation – June 2020 [Press Release]. Washington, DC: U.S. Department of Commerce; 2020, Jul 2). Available from https://www.bls.gov/news.release/archives/empsit_07022020.pdf
8. Dali'Alba G. Reframing expertise and its development: A lifeworld perspective. In K. A. Ericsson KA, Hoffman RR, Kozbelt Q, Williams AM editors. The Cambridge Handbook of Expertise and Expert Performance. 2nd edition. Cambridge: University Press; 2018. pp. 33-39.
9. Newhouse W, Keith S, Scribner B, Witte G. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST Special Publication (S.P.) [Internet]. Washington, DC: National Institute for Standards and Technology; 2017, Aug. Available from https://doi.org/10.6028/NIST.SP.800-181r1
10. Buchanan BG, Davis R, Smith RG, Feigenbaum EA. (2018). Expert Systems: A perspective from Computer Science. In K. A. Ericsson KA, Hoffman RR, Kozbelt Q, Williams AM editors. The Cambridge Handbook of Expertise and Expert Performance. 2nd edition. Cambridge: University Press; 2018. pp. 84-104.
11. Blair JRS, Hall AO, Sobiesk E. Educating future multidisciplinary cybersecurity teams. Computer, 2019, Mar; 52(3): 58-66, Available from doi: 10.1109/MC.2018.2884190.
12. Litecky CR, Arnett KP, Prabhakar B. The paradox of soft skills versus technical skills in is hiring. Journal of Computer Information Systems, 2004; 45(1), 69-76. Available from doi:10.1080/08874417.2004.11645818
13. Association of American Colleges and Universities (AACU). VALUE Rubrics [Internet]. Washington, DC: AAC&U, n.d. Available from https://www.aacu.org/value-rubrics
14. Winegard B, Winegard B, Geary DC. The evolution of expertise. In K. A. Ericsson KA, Hoffman RR, Kozbelt Q, Williams AM editors. The Cambridge Handbook of Expertise and Expert Performance. 2nd edition. Cambridge: University Press; 2018. pp. 40-48.
15. Bloomberg, L, Volpe M. Completing your qualitative dissertation: A road map from beginning to end. 3rd Edition. Thousand Oaks, CA: Sage Publications; 2016.

16. Assante MJ, Tobey D. Enhancing the cybersecurity workforce. I.T. Professional, 2011, 13(1), 12-15, Available from doi 10.1109/MITP.2011.6
17. Tobey D. Smart grid cybersecurity: Job performance model report, NBISE technical report, SGC working group, [12-01 Draft]. National Board of Information Security Examiners; 2012.
18. Haney JM, Lutters WG. It's scary … it's confusing … it's dull": How cybersecurity advocates overcome negative perceptions of security. Proceedings of the Fourteenth Symposium on Usable Privacy and Security, Baltimore: M.D.; USENIX Association, 2018, Aug 12-14, 2018. Available from https://www.usenix.org/conference/soups2018/presentation/haney-perceptions
19. Mitchell GW, Skinner LB, White BJ. Essential soft skills for success in the twenty-first century workforce as perceived by business educators. Delta Pi Epsilon Journal, 2010; 52(1), 43–53. Available from https://eric.ed.gov/?id=EJ887222
20. Creswell JW, Poth CN. Qualitative inquiry & research design: Choosing among five approaches. 3rd Edition. Thousand Oaks, CA: Sage Publications, 2013.
21. ISC(2) Cybersecurity workforce study: Strategies for building and growing strong cybersecurity teams [Internet]. Clearwater, FL: ISC(2); 2019. Available from https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study#
22. Moustakas, C. Phenomenological research methods. Thousand Oaks, CA: Sage Publications, 1994.
23. Sisson LG, Adam AR. Essential hospitality management competencies: The importance of soft skills. Journal of Hospitality & Tourism Education, 2013, Sep; 25(3), 131-145, DOI: 10.1080/10963758.2013.826975
24. Cyberseek. Cybersecurity career pathway. Interactive data set on July 7, 2020. [Internet]. Washington, DC; Department of Commerce; 2020. Available from https://www.cyberseek.org/pathway.html