Author: **Behles, Jessica E.**

Title: ***Required Skills for Technical Communicators in Cybersecurity***

The accompanying research report is submitted to the **University of Wisconsin-Stout**, **Graduate School** in partial completion of the requirements for the

Graduate Degree/ Major: **MS Degree / Technical and Professional Communication**

Research Advisor: **Dr. Gregory Schneider-Bateman, Associate Professor**

Submission Term/Year: **Spring 2019**

Number of Pages: **93**

Style Manual Used: American Psychological Association, 6th edition

☒ **I have adhered to the Graduate School Research Guide and have proofread my work.**

☒ **I understand that this research report must be officially approved by the Graduate School.** **Additionally, by signing and submitting this form, I (the author(s) or copyright owner) grant the University of Wisconsin-Stout the non-exclusive right to reproduce, translate, and/or distribute this submission (including abstract) worldwide in print and electronic format and in any medium, including but not limited to audio or video. If my research includes proprietary information, an agreement has been made between myself, the company, and the University to submit a thesis that meets course-specific learning outcomes and CAN be published. There will be no exceptions to this permission.**

☒ **I attest that the research report is my original work (that any copyrightable materials have been used with the permission of the original authors), and as such, it is automatically protected by the laws, rules, and regulations of the U.S. Copyright Office.**

☒ **My research advisor has approved the content and quality of this paper.**

STUDENT:

NAME: Jessica E. Behles **DATE: 9 May 2019**

ADVISOR: (Committee Chair if MS Plan A or EdS Thesis or Field Project/Problem):

NAME: Dr. Gregory Schneider-Bateman **DATE: 7 May 2019**

-- ----

This section for MS Plan A Thesis or EdS Thesis/Field Project papers only

Committee members (other than your advisor who is listed in the section above)

1. **CMTE MEMBER'S NAME:** **DATE:**
2. **CMTE MEMBER'S NAME:** **DATE:**
3. **CMTE MEMBER'S NAME:** **DATE:**

-- ----

This section to be completed by the Graduate School

This final research report has been approved by the Graduate School.

Director, Office of Graduate Studies: **DATE:**

Behles, Jessica E. ***Required Skills for Technical Communicators in Cybersecurity***

Abstract

The purpose of this two-phase study was to identify barriers to entry for technical communicators wanting to enter the cybersecurity field. The first phase comprised a content analysis of 100 online job advertisements for technical writers and editors in the cybersecurity field to examine the minimum qualifications sought for these positions, such as minimum education, certifications, technology experience, competencies (hard skills), and characteristics (soft skills). For the second phase, I interviewed five technical communicators already employed in the cybersecurity field to learn more about the qualifications they had entering cybersecurity, their experiences in that field, and their advice for technical communicators wanting to enter cybersecurity.

Results indicated that some positions require specialized cybersecurity or technical skills and experience, but the most important skills and qualities are generally communication based, such as writing, editing, or translating complex material into an understandable format. Government security clearances represented a barrier for some jobs, but this was mostly limited to positions with government contractors. The best way technical communicators can prepare for transitioning into cybersecurity is learning about cybersecurity and getting a command of the lingo, writing about cybersecurity topics, and practicing cybersecurity techniques—as well as maintaining their technical communication skill set.

Table of Contents

List of Figures

Chapter I: Introduction

With new high-impact data breaches being announced seemingly every month, cybersecurity (CS) is a thriving, quickly evolving field that is growing rapidly and rapidly growing in importance. Cybersecurity threats are becoming ever more pervasive and difficult to prevent. As such, the mechanisms for preventing or detecting these threats are becoming more complicated. Intuitively, it makes sense for technical communicators to be involved in ensuring that these products are usable, either by producing complete, accurate, understandable user documentation or by working alongside software developers to guide them in producing a product that is user friendly and easy to configure—after all, a misconfigured CS product can be worse than none at all.

Furthermore, many CS problems are inherently communication-based, and keeping systems and data safe is often a question of training and awareness, both in people's homes and their places of work. Technical communicators are a natural fit to face these challenges with their blend of communications skills and comfort with technology. These problems may offer technical communication (TC) practitioners opportunities to contribute to CS while also benefitting from being in a growing field with a well documented skills gap.

Purpose & Research Questions

To take advantage of these opportunities, technical communicators need to ensure that they are adequately equipped with the skills, knowledge, training, and other qualifications required to successfully transition to CS as well as continue to succeed throughout their careers in CS. Therefore, the purpose of this research is to examine CS-specific job opportunities for TC practitioners and determine the education and skills required to succeed as a technical communicator in CS. Through the research chronicled here, I will answer the following questions:

1. What relationships exist between CS and TC as reflected in the literature of both fields?
2. What types of jobs are available for TC practitioners within CS?
3. What barriers to entry will TC practitioners face?
4. What skills, knowledge, experience, and training will help technical communicators overcome those barriers and succeed in CS?

To answer these questions, I have taken a two-phased approach. First, I analyzed the contents of 100 online job advertisements for cybersecurity technical writers to determine the education, experience, knowledge, skills, and other qualifiers that hiring mangers seek for these positions. Then, for a more well-rounded perspective, I interviewed five TC practitioners already in CS to gain their perspectives of what it takes to break into CS and how to succeed once there.

This paper opens with a review of CS and TC literature that discusses the relationship between these two fields and how they can be mutually beneficial. This is followed by a description of the data collection and analysis methodologies I used for the job advertisements and TC practitioner interviews. The next section presents the results of both phases along with a discussion of the relationships and implications of the data, followed by a brief discussion of the limitations of this study. This paper then concludes with some potential avenues for additional research.

Chapter II: Literature Review

To develop a more precise understanding of the relationship between TC and CS, I reviewed and analyzed literature and publications from both fields. I began by querying UW-Stout's academic database using terms such as *cybersecurity/cyber security*, *information security*, *technical writing*, *technical communicator*, *communication*, *rhetoric*, and *security awareness*. I manually sorted through the results and selected resources that pertained to cybersecurity and writing, rhetoric, communication, or similar topics. I compiled additional resources by searching the following TC-specific publications for *cybersecurity/cyber security* and *information security*:

- *Computers & Composition*
- *IEEE Transactions on Professional Communication*
- *Intercom*
- *Journal of Business Communication*
- *Journal of Technical and Professional Communication*
- *Journal of Technical Writing and Communication,*
- *Technical Communication*
- *Technical Writing Magazine* (Techwr-l)

It may be noted that not all of these publications are scholarly in nature. Indeed, I chose to include non-scholarly sources such as trade publications within the scope of my search for two reasons. First, cybersecurity is a relatively young field with limited scholarly research (especially specific to communication), so I had to widen my search to find a larger body of sources to examine. Second, I felt that including nonacademic sources would help develop a deeper and more complete picture of how TC operates within CS. Once I exhausted these avenues, I mined the compiled articles for additional sources.

Following these searches, my compiled resources were a mix of articles from academic journals and trade publications, conference presentations and proceedings, government publications, a book, and a book review. These sources spanned from 2011 through 2018, with the exception of the book review (an outlier from 2002).

In reviewing these sources, I was able to make four major observations about the relationship between these fields.

1. The field of CS is facing problems that can be solved by knowledgeable communicators with the skill set that TC practitioners often possess.
2. Authors of CS literature seem completely unaware that TC—as a field—exists.
3. The field of TC is beginning to recognize and acknowledge its value to CS.
4. There is little guidance available for TC practitioners looking to transition to CS.

For the rest of this chapter, I will discuss these observations and their relevance to this study.

CS Needs Skilled Communicators

Sophisticated security technology (like antivirus software or firewalls) is only one part of CS—another part is the human element. Human error and poor judgment are considered among the highest risks in CS, and training and education are key in mitigating human-based risk. Several sources—written primarily from a CS perspective—focused on the challenges presented by individuals and their behaviors regarding security. Most of these challenges revolve around effectively and appropriately communicating CS risks to end users, who should be guided address those risks appropriately.

Part of the problem is that current CS education practices may be insufficient for communicating risks or the behaviors to mitigate them. In their study of cybersecurity rhetoric, Quigley, Burns, and Stallard (2015) argued that “more education in schools and at home about cyber risks will… allow people to better protect themselves and… a strong education program that engages the public might in the long term lead to the behavior change required to ensure that the benefits of cyber-space are maximized and its dangers reduced” (p. 115-116). In other words, improved CS instruction and communication—tasks familiar to TC practitioners—are beneficial due to their potential to reduce risk through more secure behaviors by individuals.

Security awareness programs are a common method of educating individuals about CS risks and teaching the proper skills to address them. However, *common* does not necessarily signify *effective*. Bada, Sasse, and Nurse (2015) bluntly stated, “The fact today is that security awareness as conceived is not working.” (p. 120). In their examination of security awareness’s failures, the authors considered the factors that contribute to successful awareness programs. They argued that “one of the most crucial parts [of a successful awareness campaign is] communication. Teaching new skills effectively can lead to prevention of high-risk online behavior, since what appears to be lack of motivation is sometimes really lack of ability” (p. 124). In other words, effective communication can both motivate and empower individuals to exercise better CS behaviors.

Yet any single individual represents a small part of the CS puzzle. One must also examine the role of the individual in the context of society, itself a decentralized network of individuals. Camp (2011) argued that “[CS] is a good that can be cooperatively produced” (p. 93) and that all of society benefits when individuals behave securely, providing collective security via digital “herd effects” (p. 94). The author suggested that one solution for increasing these herd effects is for individuals to publicly and visibly follow good security practices to normalize these behaviors across social networks.

However, Camp warned that this is impossible if these behaviors are inadequately or ineffectively communicated. Camp provided as an example the 2003 Slammer worm:

> Announcements specified that the worm attacked Microsoft SQL Server 2000, but how many users knew that their PCs, in fact, ran an SQL server? Any technically useful report could have been construed by the average user as acknowledgment that the worm did not apply to him or her. (2011, p. 99)

Because of poor communication, users often did not know their systems were vulnerable to the worm and were therefore unable to respond properly, resulting in its continued propagation to other systems. In fact, communication in CS can be so bad that “some of the language used to address computer security may, in fact, discourage compliance…. The language of computer security does not encourage norms of security adoption” (Camp, 2011, p. 104). Inappropriate or misleading language is a problem that negatively impacts the individual user as well as society as a whole.

In the Slammer worm example, poor communication practices prevented users from understanding the correct actions to take. Even more troubling, these practices have also resulted in users who have become unwilling to exercise good security behaviors. Rastogi and von Solms (2012) discussed how CS is often hampered by end users' negative feelings, preventing them “from even intending or initiating behaviors to comply with the security policies and controls" (p. 54). The solution proposed by the authors was to borrow the concept of branding from the marketing field to improve end users' perceptions of CS and thereby improve information security outcomes.

Although the authors approached the negative image problem from a marketing direction, it is still—at its heart—a communication problem. In fact, they note that “information security awareness (ISA) is already an important communication tool used… to influence end users towards compliance” (Rastogi & von Solms, 2012, p. 54). They also suggest that “to be successful, any communication program must tailor itself to the characteristics of its audience otherwise it loses its effectiveness" (p. 58). These authors have recognized the importance of communication in solving these problems, as well as indicating that audience awareness—a keystone skill within TC—is a vital part of that.

Communication problems in CS are not solely risk- or user-oriented. For instance, academic research in the field also suffers from poor communication practices. Ramirez and Choucri (2016) examined the state of academic research in CS and identified problems such as a "lack of interdisciplinary cooperation" and "a need for further refinement of standard cybersecurity terminology" (p. 2216). To address these issues, the authors argued that “the solution itself is communication. Standardizing vocabulary offers one outlet for such communication. Explaining differences in terms is another” (p. 2221). Bringing in skilled communicators to solve these problems “would accelerate the pace of research, improve policymaking and business practice, and lead to greater integration with the rest of the scientific community" (p. 2240).

Another problem that does not directly affect the end user or address risk—but is no less important—is the challenge of communicating information between audiences. Dawson and Thomson (2018) discussed the difficulty of communicating cybersecurity concepts, especially to non-technical stakeholders. “How,” they asked, “does communication occur between the Luddites and cyber workforce if the Luddites are unable to understand the technical complexity of the cyber workforce?" (p. 5). Their answer lies in a CS workforce with vastly improved communication skills. They describe an ideal workforce with skills very familiar to TC:

> Will need to be able to communicate technical information to an audience that may not have a technical background. They will need to be able to discuss requirements with budget personnel in order to obtain new resources and be able to explain to their supervisor why a certain idea may be catastrophic. If they are unable to communicate clearly, in a manner that is easily understood, they will be significantly less effective in accomplishing their critical tasks. (p. 9)

Even though the resources reviewed above focus on varying issues—from end-user behavior to standardization to CS workforce issues—they all illustrate the varied communication problems cybersecurity is facing. In fact, it is clear from this review that CS is facing some serious communication problems, which means that it has a need for skilled communicators who can solve those problems.

The solutions to these problems are equally varied, if not more so. Potential solutions to some of these problems might include:

- using audience analysis, visual design, and usability to provide effective CS training and education.
- improving end user attitudes toward CS through positive language and branding.
- increasing standardization through glossaries, style guides, and similar materials.
- translating technical information into language understandable by non-technical audiences.

This list will look familiar to most TC practitioners. After all, these solutions—and the skill sets required to carry them out—are specialties of TC. Collectively, we are experts in identifying and solving communication problems, so it follows that CS is a natural fit for TC.

CS Seems Unaware of TC

A notable feature of the sources I discussed above is that TC (or any sort of communication role) was not mentioned in any of them, despite a strongly demonstrated need for skilled communicators to solve communication problems. Even Dawson and Thomson (2018), who stated, “We lack the right personnel to communicate cyber threats to less technologically savvy decision-makers” (p. 3), apparently failed to consider (or simply did not know) that there is a whole field of personnel trained to do just that. It seems as if the authors of these sources are completely unaware that TC could contribute to the field of CS by solving these problems.

Some authors have acknowledged the need for nontechnical roles within CS. Schuster and Wu (2018), whose recent article discussed the skills required for a well-rounded CS workforce, pointed out that CS professionals who help ensure ongoing security “are a broad category encompassing technical and nontechnical jobs” (p. 1242). However, the authors did not elaborate on what comprises those nontechnical jobs, nor any indication whether they include communicators.

Similarly, the National Initiative for Cybersecurity Education (NICE) *Cybersecurity Workforce Framework*, which “strives to capture every possible cybersecurity skill or competency and sort them into specialty areas related to cybersecurity” (Paulsen, Mcduffie, Newhose, & Toth, 2012, p. 77) both acknowledges and illustrates that “cybersecurity applies to more than just traditional information assurance fields” (p. 77). This framework provides a comprehensive list of work roles (i.e., job titles) in CS; however, none of the position titles generally associated with TC (technical writer, technical editor, information designer, documentation specialist, and the like) are included among these roles. Yet more than 120 tasks, knowledges, skills, and abilities (KSAs) generally associated with TC—including technical writing!—are listed. It is unclear why the framework would include so many TC-related tasks and fail to include any TC-related job titles, but it is another indicator that CS doesn't is unaware of TC.

Additionally, several authors acknowledged that CS requires the cooperation of other disciplines and fields, and they even name some of those fields—but TC is not among them. For instance, in their article on developing a more well-rounded and self-sufficient CS workforce, Hoffman, Burley, and Toregas (2012) argued that CS should "partner with disciplines not always thought of as related to cybersecurity (for example, decision sciences, forensic sciences, public policy, and law)" (36). Dawson and Thomson (2018) pointed out that CS "is a multi-disciplinary joining of computer science, mathematics, economics, law, psychology, and engineering" (p. 1). These fields and disciplines are undoubtedly valuable to CS, but they will contribute little toward solving the communication issues it faces.

It is clear from these examples that 1) authors of CS literature understand that the field benefits from roles, skill sets, and disciplines outside CS, and 2) tasks and KSAs associated with TC are recognized by the CS field as necessary. Taken together, it appears CS recognizes its communication problems, yet remains unaware that it needs skilled communicators to solve them—and that a whole field exists that can fill that gap.

TC is Starting to Recognize its Value to CS

While CS has recognized its communication problems but not its need for communicators to solve them, is there any indication that TC has recognized and responded to this need? Some of the more TC-oriented sources (many of which are from *Intercom*, a TC trade publication) seem to indicate this is the case.

One example of TC's response to CS appears as early as 2002, in a book review published in *Technical Communication*. Zegiorgis (2002) reviewed Scott Barman's *Writing Information Security Policies* (also published in 2002). The author found the book to be "a good technical reference that information professionals will enjoy" and stating that "those in the business of technical writing will benefit" from it (p. 357). He also called out specific recommendations within the book that are especially relevant to technical communicators, showing that TC practitioners were already involved in and contributing to CS to some extent.

In a 2010 article from *Intercom*, Woelk directly addressed the topic of CS, asking, "What do technical communicators need to know about information security?" (para. 1). The article opens with "key security measures you as a technical communicator and computer user can take to protect yourself and others" and ends with a case study illustrating how a U.S. university implemented its security awareness program (para. 1). This example illustrates that TC practitioners are not only involved in CS, but are also actively working to solve some of the communication problems discussed earlier.

Similarly, TC practitioners have considered CS issues while not directly addressing CS. In a 2011 *Intercom* article, Gillenwater discussed how the increasing popularity of mobile devices (particularly tablets) has led to a need for companies to protect the data stored on (and transmitted to and from) them. The author praised the portability and usability of mobile devices, acknowledged their security risks, and provided suggestions that technical communicators can use to ensure the confidentiality, integrity, and availability (known in CS as the *CIA triad*) of the documents and data stored on and accessed via their mobile devices. Following these suggestions, she argued, would “increase the availability of your content, which will make your users happy. Securing your content while increasing your audience will ensure your company is protected, in turn making your boss happy" (Gillenwater, 2011, p. 23). Although not geared specifically for CS, this article demonstrates TC’s awareness of both the importance of cybersecurity and the TC field doing its part to increase security awareness.

Delaney and Woelk (2013) recognized that the key to security awareness is communication—and that TC practitioners, who specialize in communication and “tailoring or contextualizing our messages for our audiences,” have a clear role in security awareness and in CS as a whole (p. 10). They authors provided tips and best practices that technical communicators can use to develop effective security awareness plans. They focused primarily on the communication aspect of security awareness (including deliverables, communication channels, and messages) and identified end users and security awareness as a vital keystone of CS. Further, the authors wrote, “Security awareness and training create that awareness … much of what we do in security awareness is informing our users about cybersecurity risks and new trends” (p. 10).

In yet another *Intercom* article, McDowell (2016) discussed how communicating to end users about CS issues is vital for protecting against CS risks. She mentioned three challenges in CS communication (diverse audiences, consistency and comprehension, and timeliness versus accuracy) and presented strategies that technical communicators can use to address those challenges. Not only does McDowell’s article provide actionable recommendations for communicating CS risks to end users, but it also explicitly acknowledges the importance of communication (and therefore TC) in CS: “Communicating information about those issues is important for helping individuals and organizations protect themselves…. As our reliance on technology grows, communicating cybersecurity information to a range of audiences will become increasingly important for protecting everyone" (McDowell, 2016, p. 13-14). This article strongly enforces the notion that TC overlaps with and has much to contribute to CS.

In addition to the articles above, TC practitioners have addressed CS in presentations and national conferences. Woelk's presentation at the 2015 Technical Communication Summit provided attendees (primarily TC practitioners) updated cybersecurity advice and best practices. Finally, in 2018, Flores published her book, *The Language of Cybersecurity,* which contains definitions of for 52 CS-specific terms. Flores wrote this book as a direct response to the "communication gap in cybersecurity" and so "we can talk about cybersecurity with the same fluency that we have when we talk about other complex technical things" (Preface).

All of these examples show that TC practitioners are currently identifying and responding to the communication problems present in CS. While some provide recommendations and best practices, others clearly illustrated that technical communicators have a much wider role in CS, particularly due to a proficiency in communicating technical topics and the ability to communicate consistently and clearly with varied audiences. While CS seems unaware of the potential TC has to solve CS problems, TC practitioners have been aware and are solving problems and producing new knowledge.

TC Practitioners Lack Guidance for Entering CS

Based on the literature discussed above, there is a clear need for TC practitioners in the field of CS. The logical next step would be to see if there is any guidance available for TC practitioners who want to transition to CS. Unfortunately, current TC literature has little to offer in the way of guidance—and this seems to be the case for CS as well. In fact, as Schuster and Wu (2018) pointed out, "Despite the numerous options for individuals interested in developing cybersecurity skills through training, there is no single established career pathway" (p. 1243). Additionally, Dawson and Thomson (2018) determined that "there has been little research devoted to exactly what attributes individuals in the cyber domain need" (p. 1).

Advice is not entirely nonexistent; however, the target audience is typically CS. For instance, the NICE Framework provides a comprehensive description of the KSAs required for most CS roles. In another example, the Center for Cyber Safety and Education (2017) points out that "the top skills that are prioritized by hiring managers are communication skills and analytical skills" (p. 6), which TC practitioners have likely already mastered. Similarly, Woelk (2016) provides examples of skills required for security awareness, and these recommendations would serve just about any TC practitioner entering CS.

The good news for TC practitioners with minimal technical or CS-specific skills is that these skills may not be required to enter CS, especially for a communications-based role. In fact, Woelk (2016) wrote that "Being a successful security awareness professional does not require a technical background. Many successful security awareness professionals come from nontechnical backgrounds," (p. 6). Furthermore, he noted that 87% transitioned to CS from another career (p. 5), so those who currently want to do so will be in good company.

There was, however, one source that provided advice specifically to TC practitioners looking to transition to CS. Flores presented, "Opportunities and Strategies for Writing about Cybersecurity" at the 2018 Technical Communication Summit. In this presentation, she provided advice around the knowledge, skills, certifications, and potentially clearances that might be needed for a job in TC. This advice, based on her own experiences in CS as well as what she learned while writing *The Language of Cybersecurity*, is a good first step toward providing TC practitioners with guidance for entering CS. However, there is clearly a need for more such advice, especially data driven and evidence based.

Summary

This literature review has revealed that CS faces myriad communication problems that require skilled communicators to solve. However, it seems that CS is unaware of TC, which has practitioners with skill sets particularly suited to solving those problems. The field of TC, on the other hand, is aware of the value it can offer to CS, as evidenced by TC practitioners' involvement in CS activities and initiative in solving CS problems. This situation presents an opportunity for TC practitioners who may wish to transition to CS. Unfortunately, there exists little guidance or advice available for those who want to make the shift—and none is data driven or evidence based.

In the following sections, I will discuss my research and results, which will help fill this gap through an empirical analysis of online job advertisements and interviews with TC practitioners already in CS.

Chapter III: Methodology

This study took the form of two distinct phases: a review of online job advertisements from the site Indeed.com and a set of interviews of TC practitioners currently in CS. In this section, I will discuss the methods I used to conduct these research phases.

Phase One – Online Job Advertisements

For the first phase, I reviewed online job advertisements from the job search website Indeed.com. In TC, it is an established practice to use job advertisements as a means of assessing job prospects and employer needs within our field, and a number of authors have followed this practice (Brumberger & Lauer, 2017; Brumberger & Lauer, 2015; Lang & Palmer, 2017; Lanier, 2009; Lauer & Brumberger, 2016; North & Worth, 2000; Stanton, 2017). I drew from several of these authors' works in developing this study.

Job advertisement analysis in TC. North and Worth (2000) studied classified newspaper advertisements from around the United States to "identify trends in entry-level technology, interpersonal, and basic communication competencies and skills" (p. 144). Indeed, the authors recommended using job advertisements to determine what employers want, writing that such advertisements "remain an important resource for assessing the competencies and skills sought in today's changing workplace" (p. 145).

While North and Worth conducted their research using newspaper advertisements, subsequent researchers have turned to job advertisements posted on the Internet. Lanier (2009) studied job postings on the website Monster.com to gain perspective into the types of skills technical communication employers are seeking—with the goal of helping students prepare for these jobs. Lanier wrote, "The convenience of accessing hundreds or thousands of postings, and the rapid increase of online recruiting practices by employers, make Internet employment postings a rich and meaningful source of information" (p. 51); furthermore, "Internet employment postings can provide a window to current, employer-based needs for new or experienced technical communicators" (p. 53). In other words, Lanier found that these postings were a timely source of empirical data that can be used to provide technical communicators—both experienced and new—with research-based recommendations around what employers are seeking.

Brumberger and Lauer (2015) also analyzed Monster.com postings in their research, using their data to research the skills, competencies, and characteristics "essential for success in the technical communication market" (p. 224). Similar to the previous authors, Brumberger and Lauer found that because these advertisements "have the specific purpose of hiring an employee for a company or organization," they can provide "consistent kinds of descriptive information that can serve as a barometer of industry trends" (p. 227). These authors again used job postings for a follow-up study that focused on advertisements for user experience (UX) positions. In this article, they acknowledged that although "some degree of uncertainty is unavoidable regarding how closely the job description actually matches the day-to-day work of the person hired… it is in the employer's best interest to be as accurate, specific, and detailed as possible" (Lauer & Brumberger, 2016, p. 251). In fact, many online job search sites require companies to pay to post advertisements, further motivating employers to provide accurate and relevant information in their postings.

In another similar study, Brumberger and Lauer (2017) used job postings in three job markets to compare the skills employers seek in those markets. This study further reinforces the potential that online job advertisements can offer as a data source for researchers and job seekers alike. Finally, Stanton (2017) used job posting data in her study to determine whether writing programs are sufficiently preparing their students for the TC workplace.

The job search site Monster.com was chosen by Lanier and Brumberger and Lauer primarily due to its familiarity for the authors. Additionally, Lanier (2009) chose that site because at that time, it had “emerged as one of the most robust and widely used Internet job boards available” in addition to being familiar to him (p. 53). By Brumberger and Lauer’s 2017 article, Indeed.com had caught up with Moster.com, making them “the two most prominent job sites” (p. 214). Conversely, Stanton (2017) chose not to use Monster.com due to limitations on the site that she discovered during her time as a recruiter. Rather, she chose CareerBuilder.com, Indeed.com, and Dice.com based on her own research about, experience using, and familiarity with these sites.

Data collection. Based on the work and observations of these authors, I chose Indeed.com for my own study of online job postings. Of the options discussed in prior studies, I am most familiar with this site. Furthermore, from the perspectives of Brumberger and Lauer (2017) and Stanton (2017), Indeed.com is equal—if not superior —to Monster.com for quality and quantity of postings. Unlike Stanton, however, I chose to limit my scope to this single website for two reasons. First, like Brumberger and Lauer (2017) I wanted to avoid, as much as possible, duplicate postings. Second, Indeed.com aggregates job postings directly from employer websites as well as other job advertisement sites, including Dice.com, which Stanton also used. For these reasons, I chose to use Indeed.com for my study and no other job search websites.

To gather my data set, I performed searches on Indeed.com with four different queries: *technical writer cyber security; technical editor cyber security; technical writer cybersecurity;* and *technical editor cybersecurity.* I searched on cybersecurity and cyber security because both spellings are industry accepted, and I figured that using both would net me a higher number of valid job postings.

As for *technical writer* and *technical editor*, I followed the examples of Lanier (2009) and Stanton (2017). Lanier noted that "varying terms were often used for the occupations filled by technical communicators.… Because not all titles indicate the same profession at all locations (calls for usability experts might mean technical communication majors or cognitive psychology majors), I specified 'technical writer' to ensure unity among the positions I copied and analyzed" (p. 53). Stanton similarly used only *technical writer* for her query. This contrasts with Brumberger and Lauer (2015) who—like Lanier—acknowledged that "today's technical communicator is far more than a writer in a cubicle" and queried on more than 50 distinct job titles (p. 228). I decided that the extensive list of queries was not only beyond the scope of this study, but such a search would likely yield a large number of duplicates and comparatively little additional valuable data.

The four queries resulted in a combined total of 388 job postings. I vetted these results to cull duplicates (such as postings with different titles and companies but identical descriptions, which comprised a large fraction of the data set) and job advertisements that met the following criteria:

- overly technical or tools based
- not CS
- not TC

In excluding highly technical or tools-based job advertisements, I followed the example of Brumberger and Lauer (2015) who "discarded jobs that were focused primarily on technical/tools work rather than rhetorical work" (p. 228). In their study, examples included "complex back-end object-oriented programming languages" and "back-end coding, executing pre-existing designs, etc." (p. 228, 251). In my data set, examples included writing and managing firewall rules, developing and managing cybersecurity infrastructure, setting up and documenting network architecture, etc. These types of advertisements seemingly sought (for instance) a network engineer who happens to have writing skills, rather than a technical communicator.

I also removed any postings that were not CS—that is, not within the cybersecurity function of a company or not within a company providing cybersecurity-specific products or services. The latter resulted in a large culling due to contracting (and similar) companies that listed cybersecurity as one of many possible services offered, in which it was unclear that the position was related to cybersecurity in particular. In these cases, I made exceptions for and retained advertisements that specifically mentioned cybersecurity related duties, products, or requirements.

Finally, I culled any postings that were not TC. For the purposes of this study—and to gain a wider, more holistic view of the opportunities in cybersecurity available to technical communicators—I took a broader view of *technical communication* than implied by my original search queries. I made this decision because it has been largely accepted that technical communication encompasses domains other than technical writing. This is supported by Brumberger & Lauer's (2015) vast list of TC titles, as well as their observation that "practitioners and academics take the position that technical writers are not—and have not been for some time—just writers" (p. 225). Like these authors, I retained "jobs that emphasized rhetorically-informed writing, communication, and design skills" as well as writing-adjacent communications domains such as social media, marketing, and even assurance and auditing—

both of which require communication of technical information via reports (p. 251). My final sample contained 100 job advertisements.

Data analysis. For the first step of analyzing the data from the job advertisements, I took an approach similar to Brumberger and Lauer (2015) and extracted the following data from each advertisement:

- job title
- required education level
- required years of experience
- required certifications
- required security clearance
- citizenship requirements
- minimum qualifications

Brumberger and Lauer's research did not include certifications, clearance, or citizenship; however, my data set included numerous advertisements for government or government contractor positions with these requirements, so I chose to include them.

I then excluded from my sample any text that did not express minimum qualifications for consideration for the position, such as information about the company, employee benefits, company culture, and the like. This exercise also included removing qualifications noted as being *preferred*, *ideal*, *a plus*, or similar, because this information is less beneficial to a job seeker looking to transition to CS from another field, who will be more interested in the minimum qualifications. I also removed information about the position's responsibilities, since that information may not be a reflection of the actual qualifications required to get the job.

I adopted a similar approach to Brumberger and Lauer (2015 and 2017) in breaking up the remaining data according to products, technologies, competencies (hard skills), and characteristics (soft skills). Products are the physical (or digital) end results of rhetorical work (i.e., project deliverables). Technology refers to skills or experience in specific technologies (such as cloud, coding languages, endpoint security, access management systems, firewalls, etc.) or technology tools/programs (word processing software, project tracking software, Internet research tools, etc.).

Brumberger and Lauer (2015) defined competencies as “workplace-related capabilities… that are not explicitly tied to a technology and do not necessarily result directly in a product” (p. 235). They defined characteristics as “more abstract than professional competencies, including abilities such as analytical/critical thinking, creativity, and so on” (p. 237). I further subdivided the competencies category into TC-specific competencies and CS/IT/Other competencies. TC competencies are those typically thought of as being possessed by TC practitioners, such as technical writing, editing, communicating with subject matter experts (SMEs), audience awareness, user experience, and the like. CS/IT/Other competencies include expertise in writing specifically for CS or other domains, or expertise within CS or other domains (for instance, understanding of penetration testing methodologies or programming experience).

Once this categorization was complete, I coded the content using a hybrid methodology that started with an *a priori* codebook using Brumberger and Lauer’s (2015) code list for a starting point in the competencies and characteristics categories (p. 236, 237). I then used open coding to generate additional phrase- or word-level codes as needed for the data set. Additionally, I used open coding to generate all of the codes for the products and technology categories.

To ensure reliable coding, all of the codes were recorded in the codebook alongside examples of data I applied them to, as well as additional information to inform consistent use of the codes. The full codebook is available in 0Appendix A: Codebook.

I coded the sample in two passes. The first pass was to assign codes and refine the codebook. I used the second pass to confirm the code assignment from the first pass and correct inconsistent coding. Finally, I used a Microsoft Access database to track the codes and analyzed the complete data set with Microsoft Excel.

Phase Two – TC Practitioner Interviews

As we have seen, online job advertisements provide a good lens through which to view the competencies and experience employers are seeking. It is, however, an imperfect lens that can reveal only part of the story. For example, Brumberger and Lauer, in both of their studies, discussed the limitations of using job advertisements in this way. In 2015, they reflected that these postings' accuracy would depend on who wrote them: "The postings may have been written by those within a technical communication department or project team…. However, the ads could also have been written by personnel who are not directly involved with the position" (p. 241). Further, in 2017 they observed that they could not "be certain that the job postings accurately reflect the tasks and responsibilities of the jobs" and "cannot capture the subtleties of day-to-day practices that field research may provide" (p. 313). Taken together, these authors' articles revealed concerns about both the accuracy and granularity of online job advertisements as a data set.

Lanier (2009) also expressed concerns, questioning the reliability of postings and the methods with which they were written. He asked, "Where do [these ads] come from and how are the details within them defined? One may imagine a potential supervisor or human resources manager creating an arbitrary list of job skills… making a 'wish list' of sorts for their ideal candidate" (p. 52). Stanton (2017), who had direct experience as a recruiter, challenged Lanier's doubts and stated that the "wish list" approach to recruiting "was not the case in [her] experience as a recruiter" (p. 225).

Nonetheless, it is easy to see that online job advertisements have their limitations when it comes to finding out what employers are looking for. One solution Lanier (2009) proposed to address these limitations was "crosscheck [small samples] with the corresponding employers to find out how the ads were created and whether they truly reflect the manager's perception of what is important when hiring technical communicators" (p. 60).

Rather than approaching employers, I chose instead to interview technical communicators currently employed in CS to obtain details about the experience and skills they had when they started in CS, which could be crosschecked (to use Lanier's term) against the job ads. Additionally, I asked questions to gain insight about what ongoing education and training these individuals received after being hired, as well as the actual tasks, projects, and deliverables they worked on while employed in CS. Taken together, analysis of the job postings and data from practitioners already in CS can provide technical communicators with a detailed picture of what they might need to break into cybersecurity and succeed once they are there.

Data collection. After attaining approval from the University of Wisconsin – Stout Institutional Review Board for using human research subjects, I began seeking participants to interview. I posted requests for participants on Facebook and LinkedIn because I have a number of contacts in the TC field on both social networking sites. Specifically, I requested technical communicators who either work within the CS department of a company or work for a company that provides CS-specific products and services.

In addition to social network postings, I reached out directly to members of my personal network who might be able to connect me to participants. Finally, I searched LinkedIn for *cybersecurity technical writer* and attempted to contact potential participants who met the above criterion.

For those who responded, I provided additional information about this study, set up times and dates for the interview, and provided electronic copies of the IRB-approved implied consent form.

Participants were contacted via phone on the agreed-upon date and time. The interview—which was recorded with participants' consent—proceeded according to a number of prepared questions (which can be seen in 0 Appendix C: Interview Responses). However, where applicable, I asked additional questions to gain clarification or insight into a point or topic mentioned by the participant.

Additionally, one participant preferred to respond to the questions (which I provided) via LinkedIn message instead of a call.

Data analysis. The interviews ranged from 30 minutes to one hour. To simplify analysis, I distilled the responses based on the original question list. This was to ensure relevance and remove any extraneous data or personally identifiable information. These distilled responses are provided in 0Appendix C: Interview Responses.

It should be noted that the interviews were open-ended and organic, with the questions serving as a framework for the conversation. Although I grouped data from the interviews according to the starting questions, the participant may have provided information in a different order than that presented here.

Chapter IV: Results

In this chapter, I discuss the results of analyzing 100 job advertisements, followed by the results of the interviews with TC practitioners currently working in CS.

Job Advertisements

To present the findings from the job advertisement data, I begin with the job titles of the 100 advertisements I gathered, followed by some of the metadata found in the advertisements, such as minimum experience and education requirements. I then examine the four categories of codes identified in the previous section: products, technologies, competencies, and characteristics.

Job titles. I examined the individual job titles from each advertisement to identify relationships between the job title and other information within the advertisement. For instance, perhaps the job title could be a predictor of the level or type of experience required to qualify for the position.

Of the 100 job titles, 36 were some variation of Technical Writer (e.g., Sr. Technical Writer, Tech Writer, Tech Writer II, etc.), while 16 were some variation of Cybersecurity/Information Security Technical Writer, and three were some variation of Technical Editor. The remaining 45 were a mix of:

- more specialized versions of these titles (e.g., Senior Technical Marketing Writer, InfoSec HowTo Writer, Tech Editor/Writer [Cybersecurity Risk Management], Security Policy Technical Writer, etc.),
- other job titles typically associated with TC (e.g., Intern-Social Media, Web Content Editor, Assistant Proposal Writer, Senior UX Writer, etc.), and
- an assortment of other job titles tangentially related TC and/or CS.

The full list of job titles is available in 0Appendix B: Job Titles.

I also examined whether a given job title was generally associated with TC or CS by assigning it into one of three categories shown in Figure 1.

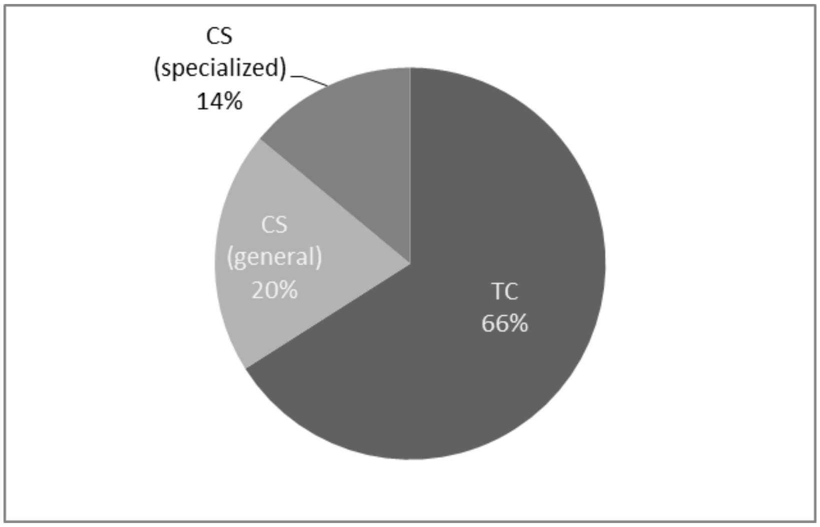

Figure 1. Relative occurrence of job titles according to categorization: *TC* (66%), *CS (general)* (20%), or *CS (specialized)* (14%).

In the figure, *TC* refers to job titles that are commonly found within TC or often associated with the field. In other words, these are your garden-variety TC positions. Examples include:

- Digital Strategist
- Technical Writer
- Instructional Designer
- Technical Editor

CS (general) refers to job titles that are more closely related to CS. This includes titles that are typically associated with TC but have a clear connection to CS. In other words, these are TC positions that appear to require some general skill or experience in CS. Examples include:

- Proposal Writer, IT Security

- Cybersecurity Technical Writer
- Information Security Instructor
- Security Policy Technical Writer

Finally, *CS (specialized)* refers to job titles that could fit in the *CS (general)* category but also reflect a specific CS or technical specialization. While still TC related, these positions appear to require specialized skills or experience in a specific CS domain, technology, or deliverable. Examples include:

- Cloud Security Technical Writer
- IT System Security Plan (SSP) Writer
- Cyber Policy & Awareness Manager
- Information Assurance Specialist
- Senior Technical Writer (Behavioral and Attack Analytics)

My goal in dividing the job titles into these categories is to make it easier to identify relationships between these positions and their qualifications. For instance, it would be reasonable to expect the *CS (specialized)* job titles to require more technical skills or knowledge (such as cloud or information assurance) than those in the other two categories. In spite of this expectation, I could not identify any relationships or correlations between the job titles and the qualifications in the job advertisements. The job titles categorized as *CS (specialized)* seemed just as likely to have technical or CS-related qualifications as the other categories.

Experience, education, and other considerations. I also extracted the minimum experience and education requirements from each job advertisement, as well as some additional requirements that should be considered when applying for one of these jobs. These considerations are:

- required certifications,
- required security clearances,
- writing samples, and
- travel requirements.

Experience. For a better idea of previous work experience required of candidates, I examined the specific types of experience required for each position advertised. I divided the listed experience requirements into the categories shown in Figure 2.

In the figure, *TC* refers to experience in the TC field or skills and tasks commonly associated with TC (e.g., “at least 5 years of experience writing technical documentation”), and *CS* refers to experience directly related to CS or IT (e.g., “at least 7 years in the information systems field”). Job advertisements that provided an experience requirement in some other field (neither CS nor IT) or was completely unspecified (e.g., “5 years of practical experience”) are *Other/Unspecified*, while those that provided no guidance for a specific number of years are *N/A*. Finally, some job advertisements specified an equal minimum number of years for two of these categories; these are reflected in the figure accordingly.

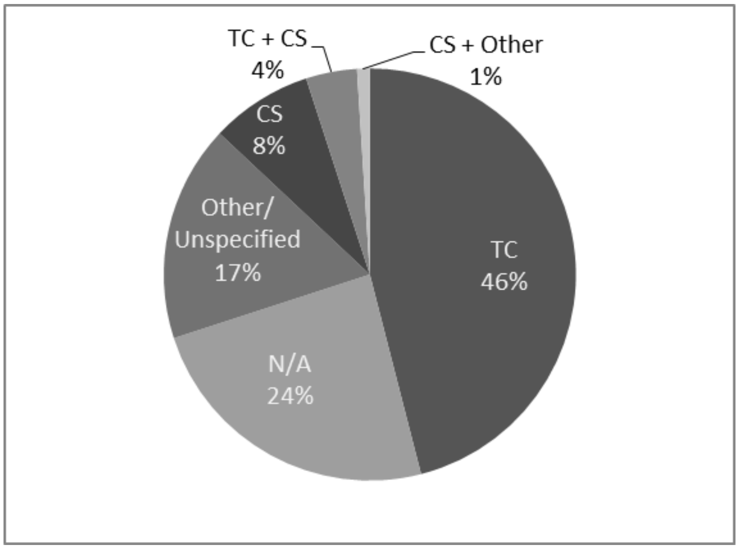

Figure 2. Relative occurrence of minimum experience according to categorization: *TC* (46%), *CS* (8%), *Other/Unspecified* (17%), *CS*, *TC + CS* (4%), *TC + Other* (1%), or *N/A* (24%).

It seems intuitive that half of the job advertisements require TC experience, but it is surprising that CS comprises such a small fraction of the sample. Even though this result is unexpected, it is consistent with Woelk's (2016) assertion that technical expertise is not necessarily a prerequisite for success in CS.

To determine how senior or junior these positions are, I also examined the minimum experience levels required, which ranged from 1 year to 12 years. Figure 3 (below) shows the number of job advertisements that listed each quantity. Around one-quarter of the advertisements did not list any year requirement. Because it was unclear whether the job required 0 years of experience or the requirement was simply unlisted, these advertisements are reflected as *N/A* rather than 0. In instances where multiple values or a range of values were listed, I included only the lowest requirement. Finally, in instances where a job listed equal requirements for two of the categories listed in Figure 2 (above), I added those values together. For instance, a job requiring six years of TC experience and six years of CS experience will be shown as twelve years.

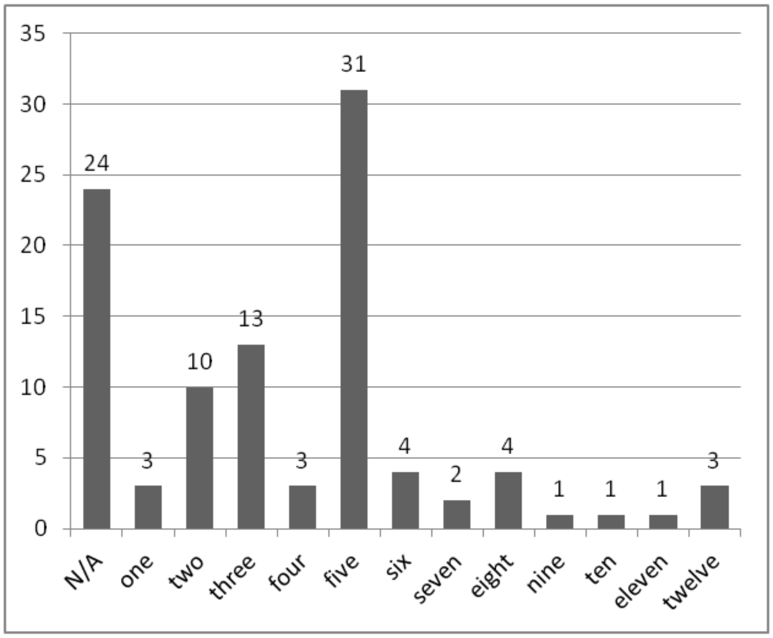

Figure 3. Number of job advertisements listing 1-12 years of experience. *N/A* indicates no minimum experience requirement was listed.

Of the job advertisements that listed minimum experience requirements, approximately a third required 5 years. Additionally, 26 required 1-4 years, while only 16 required more than 5 years. This result is good news for individuals planning to transition to CS early in their careers; however, it is also good for the more seasoned TC practitioners who desire more senior CS positions and potentially compensation commensurate with their experience.

Education. Similarly to how I categorized by field the minimum experience requirements, I also categorized the education requirements as shown in Figure 4. If the required degree was for TC or a similar major (such as journalism or English), I categorized it as *TC*; for CS or another technical major (such as computer science), I categorized it as *CS*. *Unspecified* indicates that a degree was required, but no major was included. The *N/A* category is for those job advertisements that list no degree as a requirement. Finally, while all of the degree requirements were for bachelor's degrees (65% of the advertisements called for some sort of bachelor's degree), a small number of job advertisements (mostly internships) stated that a high school diploma or GED were required—this is reflected in the *High School* category.

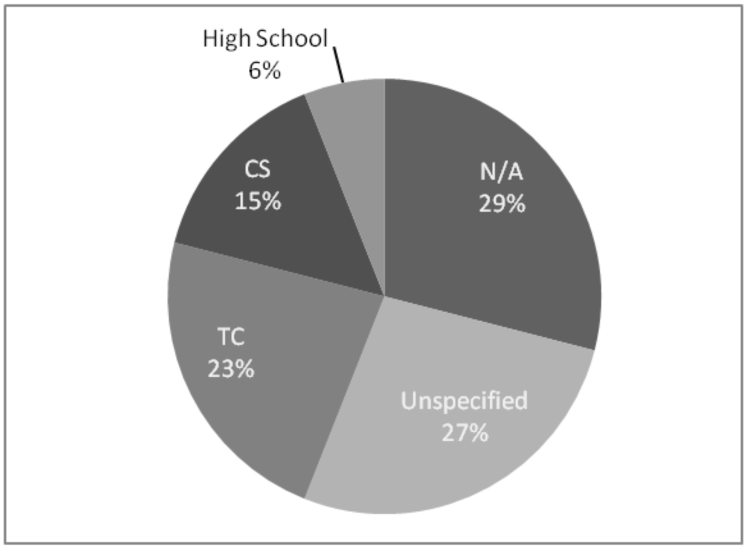

Figure 4. Minimum education levels and majors required by job advertisements. *Unspecified* indicates a bachelor's degree was listed with no specified major. *N/A* indicates no education requirement was listed.

Compared to the experience requirements, CS specialization was more desired in terms of education. However, TC is more desirable here as well. Yet in more than a quarter of the job advertisements, a degree was required but the major was unimportant. The implication is that education does not present much of a barrier as long as the applicant has some sort of bachelor's degree.

Additional considerations. In addition to minimum experience and education qualifications, I examined some additional requirements within the job advertisements. These requirements are worth noting because they could potentially act as barriers for those wanting to apply for these positions.

- Eleven of the job advertisements stated that a portfolio or writing samples were required.
- Eight required some sort of specialized CS certification. Examples include the Project Management Institute Risk Management Professional (PMI-RMP) certification, the Global Information Assurance Certification (GIAC) Security Essentials (GSEC) certification, or the Project Management Professional (PMP) certification.
- Finally, 42 of the advertisements required some sort of U.S. Government security clearance, such as Public Trust, Q, or Sensitive Compartmented Information (SCI).

Regarding the above considerations, writing samples should not present a barrier to entry, since most TC practitioners will already have accumulated a portfolio of work. Likewise, the certifications are a minimal barrier, since so few of the job advertisements listed them. The requirement for a security clearance, however, could present a major barrier. They are difficult to obtain, usually can only be obtained while already working for the government, and are required by nearly half of the sample.

Technology. As noted previously, I coded the minimum qualifications for each job advertisement with a schema that utilized four categories of codes. The technology category consists of 23 codes. These codes appear a total of 103 times across 62 of the advertisements, at an average rate of 1.03 per advertisement (inclusive of advertisements with no technology codes).

To help determine whether the job advertisements emphasized experience with CS or IT-specific technology, I divided the codes into the TC and CS/IT subcategories. I the TC subcategory to technologies or tools typically associated with TC-related job duties. I assigned the CS/IT subcategory to technologies or tools that represented some technical or CS specialization. For example, collaboration tools would be expected in an average TC job; however, hacking tools would not. Figure 5 lists each of these technology codes as well as their *frequency*—the number of job advertisements in which a given code appears.

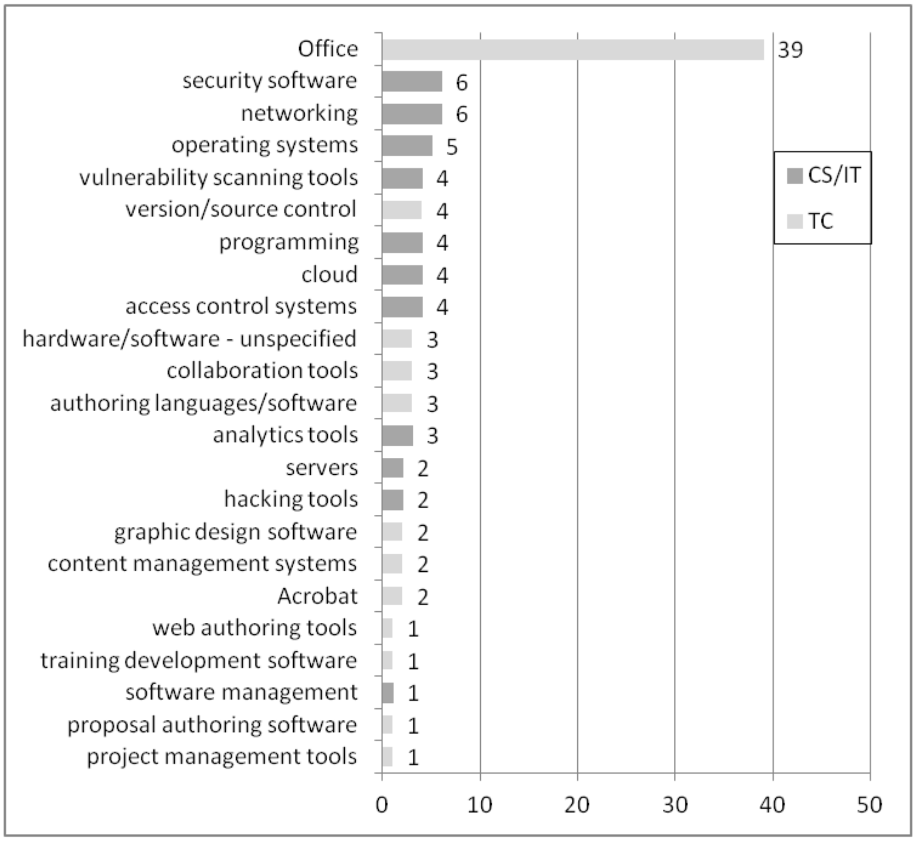

Figure 5. Frequency of 23 technology codes across 100 job advertisements, categorized as TC or CS/IT.

The *Office* code (representing any of the software in Microsoft's productivity suite of the same name, including Word, Excel, PowerPoint, Visio, SharePoint, etc.) is by far the most-used code in this category, appearing in 39 advertisements, with the rest of the codes appearing in six or fewer advertisements. These data show that outside of *Office*, there is some preference for more technical tools; however, the low frequency of these codes across the data set may indicate that specialized technologies and tools are not emphasized in this type of job advertisement.

While the figure above indicates how many of the 23 codes were categorized as CS versus IT, it does not provide the full picture. Figure 6 presents another metric, the frequency that TC codes were assigned compared to CS codes. In the figure, the left chart includes Microsoft Office (classified as a TC code), while the right chart does not.

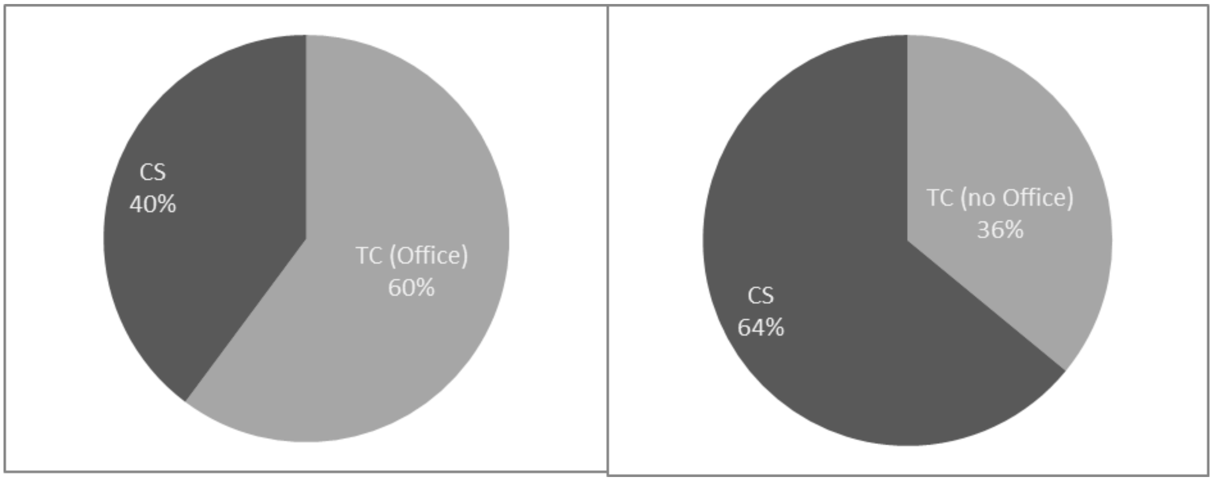

Figure 6. Total frequency of TC technology codes versus CS technology codes. Left includes *Office* code; right excludes *Office* code.

Once the *Office* outlier is removed, it becomes clear that CS codes are more dominant than TC codes. This seems to indicate that when it comes to technology and tools experience, CS employers value experience with specialized software and tools like security software or programming languages.

Products. The products category consists of 20 codes. These codes appear a total of 134 times across 54 of the advertisements, at an average rate of 1.34 per advertisement (inclusive of advertisements with no products codes).

Like the technology codes, I divided the product codes into TC and CS/IT subcategories based on whether they could be considered typical for TC or more specialized for CS (see Figure 7). The most popular codes (*procedures*, *processes*, and *policies*) are fairly common among TC positions; conversely, products like security plans and network documentation are more specific to CS.

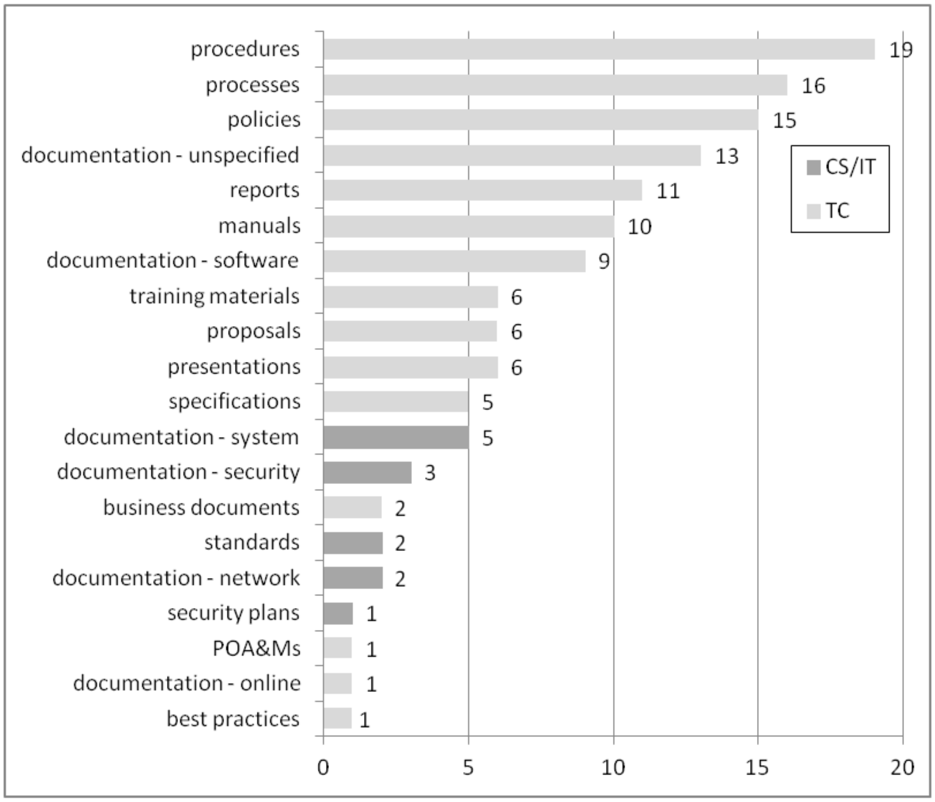

Figure 7. Frequency of 20 products codes across 100 job advertisements, categorized as TC or CS/IT.

Although this category has a smaller number of available codes than the technology category, they occur with more frequency and are more evenly spread across the job advertisements (compared to *Office*'s domination of the technology category). Furthermore, the more CS-specialized products are in relatively less demand than their counterparts in the technology category. While CS was more dominant in technology, Figure 8 illustrates that for products, TC has a much higher code frequency than CS.

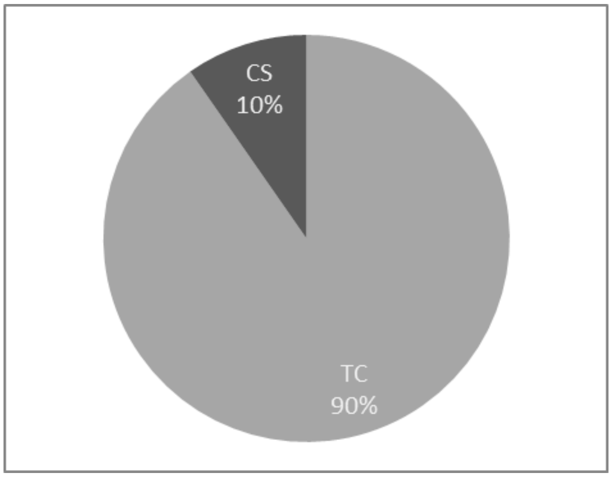

Figure 8. Total frequency of TC products codes versus CS products codes.

According to these results, TC practitioners who successfully transition to CS will be expected to produce many of the same types of deliverables that they would in a more traditional TC position.

Competencies. The largest category, competencies consists of 28 codes. Competencies also has the highest code frequency, with its codes appearing in 95 job advertisements, at an average rate of 3.91 per advertisement (inclusive of advertisements with no competencies codes). The number of codes associated with competencies may illustrate the importance of these qualifications in job advertisements.

I divided the competencies codes into three subcategories. As previously seen, the TC and CS/IT categories are based on whether they could be considered typical for TC or more specialized for CS. The third category, Other, represents codes that are not frequently associated with either TC or CS. This includes the *domain - other* code, which I assigned when the job advertisement required some domain expertise outside of TC and CS, such as auditing or financial services.

As Figure 9 shows, most of the codes are TC-related, with only two classified as CS. I assigned the *writing - CS/IT* code to a job advertisement when it required experience in cybersecurity technical writing, creating cybersecurity documentation, writing in an IT environment or for an IT domain, or similar. *Domain - CS/IT* indicates that the advertisement required either a general familiarity with cybersecurity or experience or skills in a specific cybersecurity domain, such as network security, penetration testing, or access/identity management. Figure 9 also illustrates the variety of competencies, TC and otherwise, that employers value for these types of jobs.

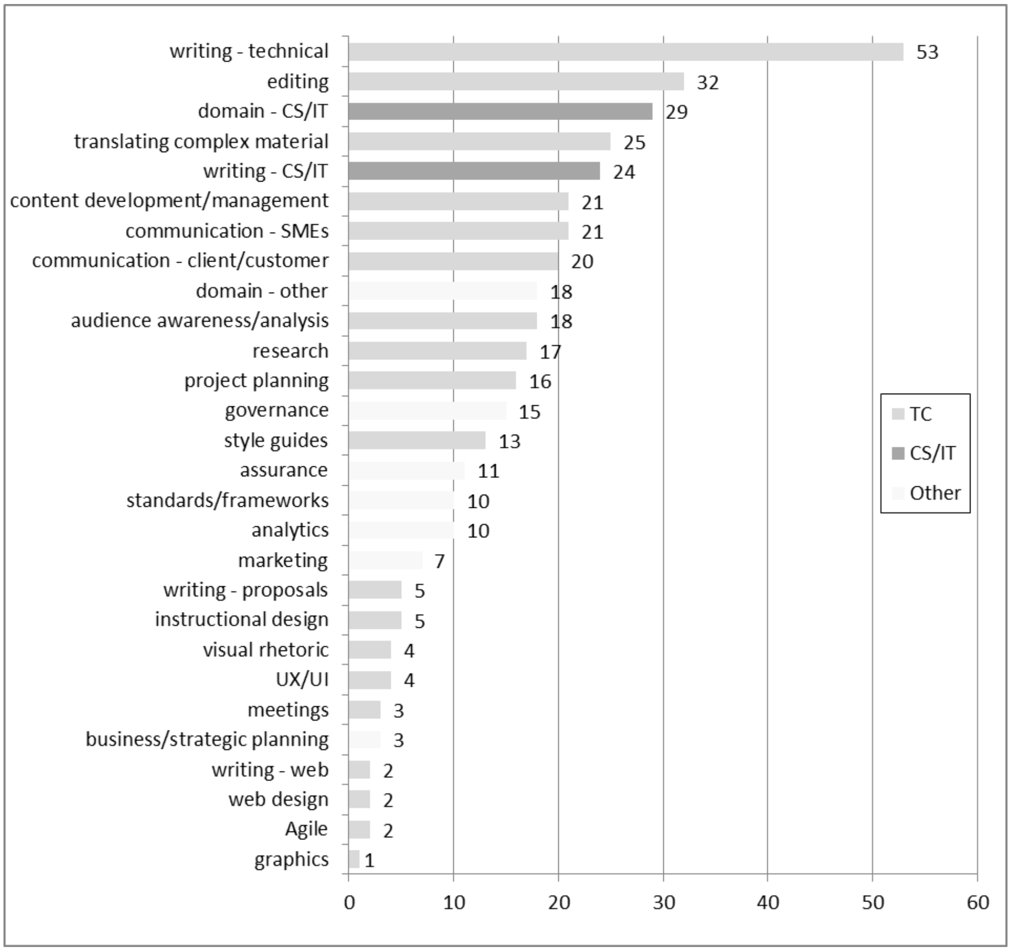

Figure 9. Frequency of 28 competencies codes across 100 job advertisements, categorized as TC, CS/IT, or Other.

Similar to Figure 9 (above), in Figure 10 (below) TC dominates this space, with TC competencies appearing at a frequency that is double the combined frequency of the CS and Other subcategories. Not only was TC dominant in this category (similar to products), but the most frequently required code was *writing - technical* by a wide margin. This could indicate that regardless of what else employers require of practitioners in these positions, they are expected to be technical communicators foremost. This is further supported by the high frequency of the *editing*, *translating complex materials*, and *content development/management* codes.

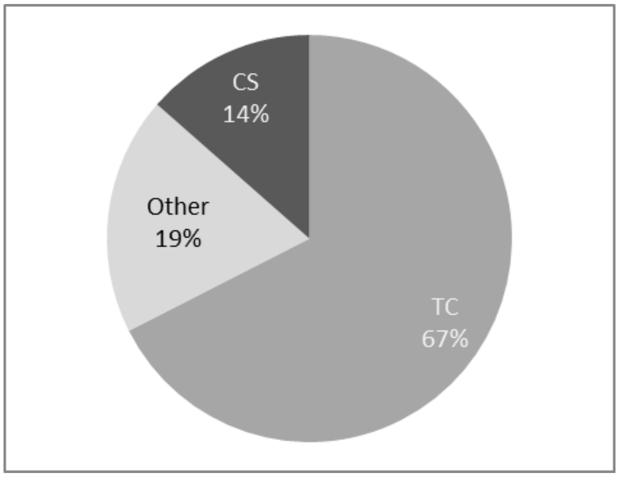

Figure 10. Total frequency of TC competencies codes (67%), CS competencies codes (14%), and Other competencies codes (19%).

Finally, 44 of the job advertisements listed no CS- or IT-specific requirements (technology or competencies codes); however, it is worth noting that many of these advertisements listed such items as “preferred.” This could indicate that specialized or technical competencies are valued, but overall considered less important than the more traditional TC competencies for these positions.

Characteristics. The characteristics category consists of only 17 possible codes and shows up in 74 advertisements. Although it is the smallest category by number of available codes, it has an average frequency of 3.24 (inclusive of advertisements with no characteristics codes), which places it right behind the competencies category. This high frequency may demonstrate that characteristics are nearly as important as competencies to employers. Figure 11 shows the relative frequency of each characteristic code.

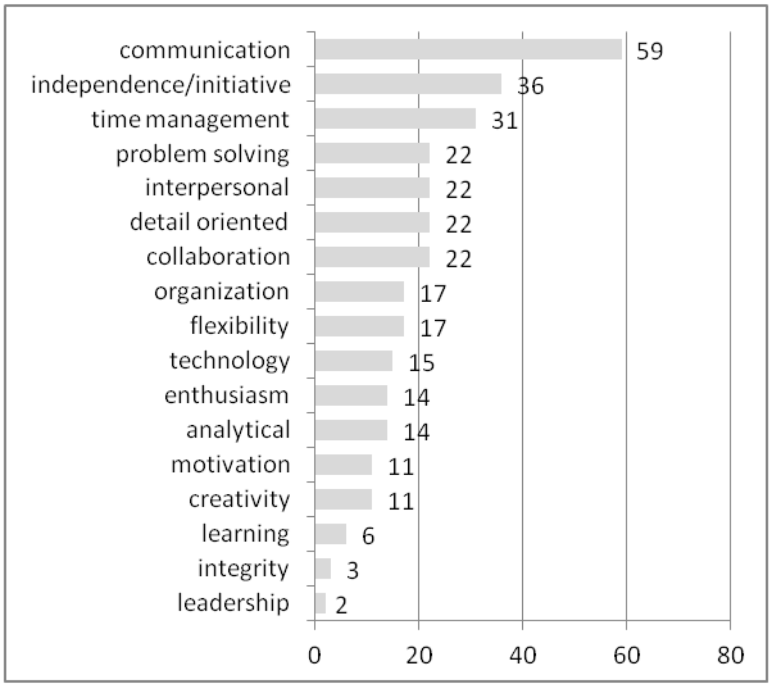

Figure 11. Frequency of 20 competencies codes across 100 job advertisements.

Communication comprises instances where the advertisement listed the ability to communicate clearly, strong verbal and/or written communication skills, a strong grasp of the English language, or similar. I have treated *communication* as a characteristic rather than a competency because job advertisements rarely treat it as an ability that is explicitly learned or taught. It is frequently listed alongside other “untaught” abilities like time management skills or problem solving skills. Lanier (2009) also treated oral and written communication skills similarly. Because writing is included in communication here, it was not included as a competency. Rather, I used the competency *writing - technical* because it is a more specialized skill that requires some training.

The *technology* code is used for instances such as willing to learn new technology, able to learn new technologies quickly, comfortable with technology, able to apply technology skills, and similar.

According to these results, the ability to communicate well is the most valued characteristic for this sample. This is no surprise, given the emphasis of TC-focused competencies and products. Furthermore, these data support the Center for Cyber Safety and Education's (2017) claim that hiring mangers prioritize communication skills when making hiring decisions.

Practitioner Interviews

I received responses from five individuals. Four agreed to participate via call, while one preferred to respond to the questions in writing (like a questionnaire) via LinkedIn message. I have compiled and summarized (for brevity) some of the results by question below; however, the full list of responses for each participant is available in 0Appendix C: Interview Responses.

Question 1: How long have you been a technical communicator in cybersecurity?

Interview participants provided the following values for how long they have been in CS, listed here from least experienced in the field to most:

- 4 years
- 5-10 years
- Almost 10 years
- 14 years
- More than 25 years

Although this information offers no direct insight into breaking into CS, the fact that each of these respondents is well established in the field lends credibility to the rest of their responses.

Question 2: Did you start from the technical communication side or the cybersecurity side? Four participants originally came from TC, while one came from CS originally. This is useful information because it demonstrates that it is possible to transition to CS from TC and (combined with the experience levels in the first question) remain successful after the transition.

Question 3: What is your current title? Interview participants provided the following job titles for their current positions, listed here alphabetically:

- Governance Risk and Compliance IT Security Policy & Procedure Writer
- Independent Security Officer
- Knowledge Base Manager
- Program Manager, Information Security Office
- Senior Cybersecurity Analyst, Governance, Risk, and Compliance

This list of job titles illustrates the variety of roles available in CS. Interestingly, only one of these titles includes any reference to writing, given that variations on *technical writer* comprised the bulk of the titles in my job advertisement analysis.

Question 4: Please briefly discuss your current role and duties. Interview participants responded with a variety of duties associated with their roles. These duties align quite well with the competencies compiled as part of the job advertisement analysis. Some examples include (listed alphabetically):

- Building a security awareness program
- Coaching
- Communicating with customers/SMEs
- Content management

- Governance and oversight
- Instructional design
- Maintaining/patching/troubleshooting systems
- Project planning/management/strategy
- Quality assurance
- Social media
- Technical writing and editing
- UX/UI

These responses reflect a mixture of TC duties and CS duties; however, there seems to be more emphasis on the duties that are more traditionally within the TC domain. This is consistent with the job advertisement analysis, where there were more competency codes in the TC subcategory in addition to those codes having a higher frequency across the advertisements than the CS codes. The interview results also align with the job advertisements in that there exist roles where the practitioner may be called upon to perform more specialized CS or IT duties (such as maintaining computer systems).

Question 5: What projects and/or deliverables do you work on/produce most often? This question and its responses align with the products category of codes from the job advertisement analysis. Some examples include (listed alphabetically):

- Documentation prototypes
- Incident response plans/disaster recovery plans
- Memos
- POA&Ms
- Policies, standards, procedures, guidelines

- PowerPoint presentations
- Reports
- Security documentation
- SOPs
- Style guides
- Technical writing: installation manuals, user guides, troubleshooting guides, etc.
- Templates
- Test plans
- Training materials
- Web content

Similar to question 5, the responses to this question are very consistent with the data from the job advertisement analyses. That is, the majority of the deliverables reported by the interview participants are typically associated with TC, while a small number CS oriented (such as security documentation).

Question 6: Can you discuss how you ended up in cybersecurity? Three participants were referred by a friend or coworker. One participant was contacted by a recruiter. One participant stepped into the role to solve a problem.

These responses are interesting because they imply that these practitioners were not actively seeking a position within the CS field. This may be an indication that CS does indeed recognize the roles that TC practitioners could play with regard to solving communication problems, as discussed in the literature review of this paper. It is unclear whether this revelation disproves the trends I discussed in that section, or if it is part of a natural evolution toward the realization that TC can solve CS problems and taking appropriate action in seeking out TC practitioners to solve them.

Question 7: While in your current position, have you had any cybersecurity-specific education or training? If so, please describe. Four of the participants had no previous CS or IT education or training. The remaining participant had a bachelor’s degree in an IT-related field. These responses are consistent with the results of the job advertisement analysis, in which the majority of advertisements listed no specific CS or IT training among their minimum qualifications.

Question 8: While in your current position, have you had any cybersecurity-specific education or training? If so, please describe. Three participants earned their Certified Information Systems Security Professional (CISSP) certifications while on the job; one also received the Security Essentials Global Information Assurance Certification (GIAC GSEC) in addition to the CISSP. One participant earned the Cisco Certified Network Associate (CCNA) certification while on the job. One reported no CS education or training.

Question 9: Was the position contingent on that training? Of the four participants who reported that they earned CISSPs, two stated that the certification was required either to maintain a current position or be promoted.

Question 10: Do you plan to continue cybersecurity-specific education and training? While one participant reported that no additional CS education would be pursued, the other four said they were planning or considering additional CS-specific education, training, or certifications. One participant provided no additional details, while one stated that only informal training, such as self-education or conference attendance, was planned. Participants named the following specific certifications as ones they were pursuing or considering pursuing:

- Amazon Web Services (AWS) SysOps Administrator
- Certified Ethical Hacker (CEH)
- Certified Information Systems Auditor (CISA)
- CISSP
- Project Management Professional (PMP)

Question 11: Is ongoing cybersecurity education required for your role? Only one participant reported that ongoing cybersecurity education was required for his or her role.

The responses to questions 8-11 seem to indicate that on-the-job CS-specific education or training may be the norm, whether or not it is required for the position. One data point that would make these results more meaningful would be whether this training was provided by the participants' companies, or whether they had to pay out of pocket. Unfortunately, I did not think to ask that question as part of these interviews.

Question 12: Do you think that cybersecurity-specific education or training has been beneficial to your role? Although only four of the five interview participants reported receiving CS education or training after being hired, all four found it beneficial. Four distinct themes rose from these responses.

A better understanding of CS. Three participants made comments that training provided them a better understanding of CS. One respondent mentioned that their role was on the more technical side, so the additional education was especially useful. Another said, "It made me feel much better in terms of knowing I understood the subject matter better."

Improved relationships with SMEs. Three participants felt that gaining a better understanding of CS improved their relationships with SMEs and other "technical folks." They felt that it broke down the technical language barrier, gave them more credibility, and improved rapport. One respondent spoke very highly of the effect of a certification on SME relationships:

> All of a sudden the engineers were a lot more willing to talk to me. Because before they thought I was just one of those "English teacher" type technical writers who didn't have a clue about technology, but was pretty good with knowing where the apostrophes and commas are supposed to go. But by having a CCNA, all of a sudden I could walk in and talk to the engineers, and they were like, “Wow, you're one of us!”

Up-to-date information. One participant said the biggest benefit of ongoing CS education was being able to stay up to date with “trends and emerging requirements.”

Increased marketability. One participant felt that training and certifications were beneficial for improving one’s marketability.

Even though continued CS education was not required for most of these individuals, they all found it beneficial in their roles. This information implies that TC practitioners who have transitioned into CS may be more successful if they pursue CS training, education, or certifications.

Question 13: Please briefly discuss your education and training outside of cybersecurity. Interview participants all possessed at least a bachelor’s degree in a non-CS subject, listed here in no particular order:

- Bachelor’s in journalism
- Bachelor’s in English; Master’s in TC; PhD in TC (in progress)
- Master’s in library and information science
- Bachelor’s in biology
- Graduate-level technical writing certificate

These results are consistent with the job advertisement analysis, in which half of the positions required a bachelor’s degree either in TC or no particular major.

Question 14: What cybersecurity-specific skills and/or tools do you use most often? This question aligns with the technology category of codes from the job advertisement analysis; however, the responses here only focus on the CS-specific technologies, while the advertisement results have both TC and CS. Some examples of responses include (listed alphabetically):

- Analytics tools
- Firewalls
- Managed security service providers (MSSP)
- Network scanning and packet analysis
- Passwords/access controls
- Ransomware
- Server hardening
- Virtual private networks (VPNs)
- Vulnerability scanning/management

The responses to this question feature some specific technologies and skills that were not reflected in the job analysis and vice versa. This could have a number of reasons, including a lack of granularity in coding, the small sample sizes, or simply the fact that CS is a large field that uses a wide variety of specialized technologies and tools. Regardless, these responses are consistent with the job advertisements in that some specialized technical skills may be required of those who transition to CS.

Question 15: What advice do you have for somebody wanting to become a technical communicator in cybersecurity? The participants responded with a variety of actionable advice for TC practitioners who want to break into CS. There was a surprising amount of overlap between the responses to this question. Several distinct themes surfaced among the advice provided.

Learning about CS. All five participants recommended education. The general consensus was that formal degrees and certifications are good for marketability ("An entry level certification in cybersecurity also helps a lot."), but not required. The key is to gain a basic, but thorough, grasp of CS concepts and topics to "[get] a baseline understanding" of the field. In particular, a strong understanding of CS vocabulary is necessary to succeed and communicate with others, including SMEs, vendors, regulators, executives, and others. Keeping up with the field, such as emerging trends, technologies, or threats, is also important.

Participants suggested several ways to gain this education beyond formal education or certification programs. Examples included attending CS-specific conferences, following CS trade publications, and becoming familiar with some of the CS-specific regulations and standards.

Writing about CS. All five participants also indicated that it is vital to practice writing about CS issues and topics both before and after transitioning to the field. This helps TC practitioners in a number of ways, such as gaining expertise in specific topics that interest them, producing writing samples to demonstrate that expertise (build credibility), making some additional money on the side, and even simply practicing good writing skills.

One participant said, "They have to try writing something. You'll need writing samples. A blog, even if nobody reads it, can show you know what you're talking about and could help you get through the door." In addition to blogging, participants suggested publishing articles on LinkedIn or in a trade magazine, writing on a volunteer basis, and freelance writing gigs.

Practicing CS. Another part of increasing subject matter expertise and preparing to transition to CS is to practice CS. This means not just writing about CS topics, but actually practicing using the technologies that might be encountered. One participant made the following recommendation:

> [If you're interested in AWS], look at AWS security and get a free AWS account and just play around with some of those things. [If you're interested in penetration testing], get the Metasploit book, download Metasploit, and get some fluency with what these tools look like…. and suddenly the light bulb will go off.

In other words, TC practitioners should choose a technology that is interesting and actually start using it. And then, ideally, write about it.

Maintaining TC skills. The participants all indicated that while CS expertise and practice is important, it is equally vital for practitioners to maintain their TC skills. One participant responded, "Computer science or domain-specific education might help get your foot in the door, but education and experience with writing and editing (communicating complex information about cybersecurity topics to many different audiences) is going to be more useful as a technical writer." Another recommended, "First of all, just be darn good at English grammar, spelling—eagle eyes for finding typos—organization, syntax, that type of thing."

These responses are consistent with the job advertisements and the literature review in their emphasis on the importance of communication skills. This makes sense because TC practitioners are needed to solve communication problems—it is only logical that they would need to be skilled in communication above all else.

Question 16: Do you have any other comments that you'd like to make? Several of the interview participants expressed high levels of satisfaction while illustrating optimism about the future of technical communication practitioners in CS. For example, one participant said, “It's such a huge growth field for us. It's a great spot. I think it's a great area for TC to go into…. It's a vibrant, growing, rich field… the pay's good…. It's growing more and more complex, so there's more and more work to do. It's a growth field, and I think that's important.” Other participants’ responses reflected similar sentiments, including another who praised the income potential of CS.

Responses also indicated that TC has, and will continue to have, a place at the CS table. Part of this is due to the ever-increasing need for CS (“If you're interested in any field--even if it's not cybersecurity--there is a need for cybersecurity. [Everyone] needs [CS].”), and part is because in CS, “our biggest issue is still people, and people understanding what they need to be careful of and training them to recognize things and know how to deal with them.”

Participants were also optimistic about future prospects within CS. As I discussed in my literature review, companies have recognized a need to solve communication problems, but are not always sure how to solve them—and may not even know about TC and what it could contribute toward solving these problems. One participant said, “It's obvious that the people asking for tech writers do not have a clue what a tech writer is…. They have no clue what they need; they just have a bit of pain, but somebody told them they need a tech writer--but they have no clue what a tech writer does.” The same participant also observed that there is a lot of competition for traditional TC jobs, but “in [CS], there's a lot less competition because tech writers haven't figured out that this area is even here.”

Further, one participant who makes hiring decisions expressed frustration that it was a struggle to find qualified candidates for even entry-level technical writer positions. The basic qualifications were a bachelor’s degree in any field, proven skill in technical writing, and “some interest and knowledge in working with software or technology. It doesn't seem like a lot, but finding those two things is actually more difficult than I expected.” In other words, the well documented talent gap that affects the rest of CS also exists for the TC positions within CS.

These insights are valuable for any TC practitioner interested in transitioning to CS. This information would generally not be reflected in job advertisements, so this study illustrates the importance of getting insight from those already in the field in addition to reading job advertisements.

Chapter V: Discussion

I will now discuss in more depth the results I presented in the previous section. I will begin with some comparisons between my results and those of previous surveys of job advertisements, followed by a discussion of how some of the specialization required in these advertisements may present barriers to entry for technical communicators. I will then discuss in more depth how the practitioner interview responses compare to the results from my job advertisement analysis. Finally, I will discuss the implications of this research for TC and CS and close with a brief discussion of the limitations of this study.

Job Advertisements

Following is a discussion of the results of the results from the online job advertisement analysis.

Relationship with previous studies. At this time, it is appropriate to discuss my results in comparison with others' for similar studies, to see whether job advertisements specific to the CS field differ from advertisements for less specialized positions in TC.

In terms of education requirements, in my results, 65% of advertisements required a bachelor's, but none required anything higher. In comparison, Brumberger and Lauer (2015) found that 57% of job advertisements required a bachelor's degree, with some of the more specialized postings requiring a master's or higher (p. 231). In Stanton's study, 65% of advertisements required a bachelors, while 3% required a master's or higher. The similarity is notable, and it would be interesting to see a breakdown of those studies' results to determine if any specialized degrees were required (like in my data, where 15% required some sort of CS- or IT- specific degree), or simply having any type of bachelor's degree was sufficient.

My results for required years of experience were very similar to Brumberger and Lauer's (2015). Both data sets reflected both 5 years and 2 years as common requirements; however, their data have a higher number of jobs requiring 2 years' experience, whereas my data have more requiring 5 years' experience. This may be reflective of the more specialized nature of the advertisements I studied, since in some cases they required experience in both TC and CS.

Surprisingly, translating complex material, which appeared quite frequently in my data set, was fairly uncommon in Brumberger and Lauer's (2009). Their results for subject matter familiarity (which align with my *domain - CS* and *writing - CS* codes) are also lower than I had expected. Perhaps these differences can also be attributed to the more specialized and technologically inclined nature of my sample.

Demand for Microsoft Office and similar tools was very high across my data as well as Lanier's (2009), Brumberger and Lauer's (2015), and Stanton's (2017). Similarly, job advertisements across all four studies demonstrated high demand for technical writing skills and communication skills. While there are no surprises here, the consistency in these results does help validate my own data and observations.

Even though the job advertisements I targeted were more specialized than those in Brumberger and Lauer's (2015), Lanier's (2009), and Stanton's (2017) studies, their results are in line with my own. All identified subject matter specialization as having some importance for the position being advertised. Furthermore, all four studies showed that experience with technology outside of Office seems to be less important to employers than other considerations and qualifications.

Despite differences in methodology, sample size, and specialization, it appears that my results do not differ all that much from other studies of TC job advertisements. Compared to

Lanier (2009), Brumberger and Lauer (2015), and Stanton (2017), my results reflected specialized qualifications—such as specific degrees, technology expertise, or specialized experience—but the basic requirements seem fairly in line with others' results. This has positive implications for those interested in breaking into CS.

Specialization. As mentioned above, while my results were in line with those of similar studies, the job advertisements I examined did require a bit more specialization in education, experience, and skills. For instance, 13 of the job advertisements I examined required at least 1 year of experience in CS or IT, 15 required a CS- or IT-specific degree, 21 required experience with some CS-specific technologies, and 47 required CS writing or CS subject matter expertise. Additionally, eight of the job advertisements listed CS certifications as requirements. (Interestingly, all but one of the jobs requiring certifications also required a government clearance.)

Taken together, all of these qualifications do pose a barrier to technical communicators wanting to enter the field, but it is less of a barrier one might anticipate. Even accounting for all of the requirements listed above, more than one-third of the job advertisements I studied required no education, previous experience, technology skills, or competencies related to CS.

Practitioner Interviews

Following is a discussion of the results of the results from the practitioner interviews.

Compared to job advertisements. One might be surprised to note that the responses from the four practitioners I interviewed (as well as the one who submitted answers in writing) have strong parallels with the job advertisements. All of the participants had some sort of education (usually a bachelor's) prior to entering CS, which seems to be the minimum "price of entry." Similarly, most participants had little to no prior experience, education, or skills in CS prior to entering the field, but they all had strong communications skills. This, too, is in line with the job advertisements, which emphasized the importance of communication skills—particularly those related to technical writing—over more specialized CS skills. As far as those skills go, the general consensus among the interview participants was that those skills can be gained as needed, along with any necessary certifications and training.

One interesting contrast between the interviews and the job advertisements was that the latter emphasized soft skills (characteristics), while they were hardly mentioned by the interview participants. The exceptions to this (outside of communication, which I discussed in the previous paragraph) were several responses that called out the importance of being comfortable with technology and able to learn new software or technology quickly. It is easy to see why such a skill would be so important to technical communicators in any field, so it is surprising that the job advertisements failed to call it out more as a necessary skill.

The products were quite similar between both data sets, as were the competencies and tools, illustrating an unexpected amount of alignment between the qualifications in the advertisements and the actual job duties of the practitioners. This may mean that the job advertisements are more accurate than detractors like Lanier (2009) have implied.

Implications for TC and CS

To briefly recap, the purpose of this research was to determine:

- the relationship between TC and CS,
- available jobs for TC practitioners within CS,
- the barriers TC practitioners will need to overcome, and
- the knowledge, experience, and training required to overcome those barriers.

For the first item, the literature review established that CS has communication problems that TC practitioners are particularly suited to address; however, the CS field seems completely unaware that the TC field has the resources to assist with these problems. While the results of this research may make it easier for TC to break into CS, it seems that there needs to be additional work on the CS side to bridge the gap between the two fields and make CS aware of these resources. Hopefully, this research helps bring the two fields closer.

This research has established that there exists a variety of jobs for different experience levels within CS for which TC practitioners are a good fit. Furthermore, the barriers to entry for these jobs remain relatively low; many of the positions analyzed required only a bachelor's degree and a skill set largely geared toward the communication skills that most TC practitioners will already possess. Some of the positions do require security clearances, which can be difficult to obtain if one is not already employed in some capacity for the U.S. government.

This research directly benefits TC through enabling evidence-based recommendations to assist TC practitioners in breaking into CS. This will also benefit CS if it results in more TC practitioners transitioning to CS and using their skill sets to solve the field's communication problems.

Limitations

This section discusses some of the limitations of this research and the methods used herein. First and foremost is the small sample size. A sample of only 100 job advertisements cannot be considered a statistically significant representation of the whole body of TC/CS job advertisements. However, it is my hope that the sample is large enough to serve as a snapshot or lens one can use to view the needs of these employers in this field.

Another consideration is the fact that—unbeknownst to me initially—Indeed.com is apparently heavily used by U.S. Government agencies and their contractors. This fact became clear to me as I began to analyze the data and identify the number of positions requiring security clearances. It is not clear that the high proportion of these advertisements is normal for the field or just this particular job board. It is also unclear whether these jobs skewed the data, or if a similar study focusing only on private-sector positions would have similar results.

Finally, there are some potential limitations with the interviews as well. Much like the job advertisements, this part of the study suffers from a small sample size. Furthermore, an ideal study would involve a random sample of participants, whereas all of the participants in this study were self-selected individuals. Additionally, each of the participants was an established mid-level or senior professional who had been in CS for some time. Despite my best attempts, I was unable find participants at earlier stages in their careers (perhaps interns or entry-level).

Chapter VI: Conclusions and Additional Research Avenues

Taken together, the data from the job advertisements and the practitioner interviews paint a picture of CS as a dynamic, growing, and challenging field with many opportunities for the technical communicator who is capable of learning some specialized skills and perhaps pick up a certification if he or she has the resources. Furthermore, while there are some barriers to entry, there are fewer than I think most people would expect—indeed, prior to this research, I thought it would be much more difficult for a TC practitioner to break into CS.

The study and results described in this paper have been used to provide guidance and advice to technical communicators wishing to overcome those barriers and transition to CS. This guidance ultimately boils to learning about CS, writing about CS, and practicing CS while not neglecting one's original TC skill set. The TC practitioner already in CS can succeed within this field by following this same advice while also taking advantage of any employer-offered training, education, or certification opportunities.

This research serves merely as a starting point for not only TC practitioners interested in CS, but also for both fields collectively. There is almost no research about the benefits TC can offer CS, minimal guidance and few best practices for processes or deliverables completed by technical communicators in CS, and almost no rhetorical analysis of the work going on in the overlap between these fields.

Even relative to my own research here, there are a number of opportunities for research around how TC practitioners can break into CS and the work they will do once there. If anything, this research could be viewed as a pilot due to its small sample size and limited scope. For instance, my study did not examine or compare opportunities between different industry sectors or even private sector versus government jobs—from my limited observations, government jobs do have different requirements, especially around certification. Even simply using a different job board may yield interesting comparisons. Another potential research direction would be to interview TC practitioners who more recently transitioned into CS, as compared to my participants, who generally had more senior positions. Finally, a particularly useful direction for research would be case studies around how TC practitioners are specifically addressing the various communication challenges presented by CS.

Moving forward, I hope that my research inspires and enables more technical communicators to transition to CS and inspires other researchers to examine this dynamic, growing field.

References

Bada, M., Sasse, A., & Nurse, J. (2015, February). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*. Coventry, UK: Cornell University.

Brumberger, E., & Lauer, C. (2015). The evolution of technical communication: An analysis of industry job postings. *Technical Communication, 62*(4), 224-243.

Brumberger, E., & Lauer, C. (2017). International faces of technical communication: An analysis of job postings in three markets. *Technical Communication, 64*(4), 310-327.

Camp, L. J. (2011). Reconceptualizing the role of security user. *Daedalus*, *140*(4), 93-107.

Center for Cyber Safety and Education. (2017). 2017 *Global information security workforce study: Benchmarking workforce capacity and response to cyber risk*. Retrieved from https://iamcybersafe.org/wpcontent/uploads/2017/06/Europe-GISWS-Report.pdf

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, 9, 744.

Delaney, C., & Woelk, B. (2013). Engage! Creating a successful security awareness program to reduce risk. *Intercom, 60*(6), 9-12.

Flores, T. (2018). Opportunities and strategies for writing about cybersecurity [Presentation slides]. *STC Technical Communication Summit 2018*, Orlando, FL.

Flores, M. A. (2018). *The language of cybersecurity*. Laguna Hills, CA: XML Press.

Gillenwater, J. (2011). Mobile devices improve security options: Improving availability while maintaining confidentiality and integrity. *Intercom, 58*(9), 22-23.

Hoffman, L., Burley, D., & Toregas, C. (2012). Holistically building the cybersecurity workforce. *IEEE Security & Privacy, 10*(2), 33-39.

Lang, S., & Palmer, L. (2017). Reconceiving technical editing competencies for the 21st century: Reconciling employer needs with curricular mandates. *Technical Communication, 64*(4), 297-307.

Lanier, C. (2009). Analysis of the skills called for by technical communication employers in recruitment postings. *Technical Communication, 56*(1), 51-61.

Lauer, C., & Brumberger, E. (2016). Technical communication as user experience in a broadening industry landscape. *Technical Communication, 63*(3), 248-264.

McDowell, M. (2016). Overcoming cybersecurity communication challenges. *Intercom, 63*(3), 13-14.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017, August). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800-181).* National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-181

North, A., & Worth, W. (2000). Trends in entry-level technology, interpersonal, and basic communication job skills: 1992–1998. *Journal of Technical Writing and Communication, 30*(2), 143-154.

Paulsen, C., Mcduffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy, 1*0(3), 76-79.

Quigley, K., Burns, C., & Stallard, K. (2015). ‘Cyber Gurus’: A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly*, *32*, 108-117.

Ramirez, R., & Choucri, N. (2016). Improving interdisciplinary communication with standardized cyber security terminology: A literature review. *IEEE Access*, *4*, 2216-2243.

Rastogi, R., & von Solms, R. (2012). Information security service branding: Beyond information security awareness. *Systemics, Cybernetics and Informatics, 10*(6), 54-59.

Schuster, D., & Wu, S. (2018). Toward cyber workforce development: An exploratory survey of information security professionals. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 62*(1), 1242-1246.

Stanton, R. (2017). Do technical/professional writing (TPW) programs offer what students need for their start in the workplace? A comparison of requirements in program curricula and job ads in industry. *Technical Communication, 64*(3), 223.

Woelk, B. (2010). Digital self defense for technical communicators. *Intercom, 57*(9), 6-9. Retrieved from https://www.stc.org/intercom/2010/11/digital-self-defense-for-technical-communicators/

Woelk, B. (2015). The secure communicator: Protect yourself and your client [Presentation slides]. *STC Technical Communication Summit 2015*, Columbus, OH. Retrieved from https://benwoelk.com/presentations/

Woelk, B. (2016, August 10). The successful security awareness professional: Foundational skills and continuing education strategies [Research bulletin]. *ECAR*. Retrieved from https://library.educause.edu/resources/2016/8/the-successful-security-awareness-professional-foundational-skills-and-continuing-ed-strategies

Zegiorgis, S. (2002).   Writing information security policies [Review of the book Writing Information Security Policies by S. Barman. *Technical Communication, 49*(3), 357.

Appendix A: Codebook

Technology Codes

Office	Anything Microsoft Office (Visio, PowerPoint, excel, word, SharePoint, etc.) or similar functionality with those tools (OpenOffice, Google Docs, etc.)
networking (CS)	Experience with some of the following networking protocols: Common Industrial Protocol (CIP), EtherNet/IP, ControlNet, and DeviceNet Familiarity with automation hardware. Firewalls, routers, gateways
Acrobat	Adobe acrobat
version/source control	Ability to use source control tools such as Bitbucket to edit comments in source code.
analytics tools	Analyzing data and building reports (charts/dashboards)
authoring languages/software	Experience with web authoring tools such as XML, HTML, Markdown
graphic design software	Adobe Photoshop, and Illustrator.
vulnerability scanning tools	
servers	
security software	Tools and software used to increase security posture
content management systems	
operating systems	Linux, Windows,
hacking tools/ methods	Tools and software used for security research or penetration testing (Metasploit, Kali Linux)
proposal authoring software	
software management	
aloud	
access control systems	Active Directory, single sign on, authentication, access policies, identity management, PKI, credentials
training/development software	
hardware/software - unspecified	
collaboration tools	
project management tools	
Web authoring languages/software	
programming	Writing code, interpreting code, programming languages

Products Codes

policies	
best practices	
processes	Workflows, processes, flow charts
standards	
procedures	
documentation - system	
manuals	Manuals, quick start guides, help content
training materials	Curricula, computer-based training, training content, training modules
proposals	
documentation - online	
documentation - network	
documentation - unspecified	
documentation - security	
Documentation - software	Including APIs
security plans	
POA&Ms	Plans of actions and milestones
presentations	Creating artifacts related to presentations (slide decks, minutes, notes, attendance)
business documents	
specifications	
case studies	

Competencies (hard skills) Codes

audience awareness/analysis	"• An advocate for customer needs."
writing - technical	
business/ planning	"Assisting with long-range planning in support of existing and projected organizational mission requirements."
communication – client/customer	
content development/management	"define, build, and execute on a documentation strategy from the ground up" "Ability to create new complex technical documents" "Experience structuring documents and maintaining version control within a technical team" "Experience producing and organizing content" "Ability to develop communication schedules, plan distribution strategies, create review

	processes” “Skilled in consolidating input from many sources into one final cohesive piece of content”
editing	Editing, proofreading, revising, providing feedback, reviewing
project planning/management	“• Experience with managing due dates and tracking deliverable items to the customer” “leading projects” “Demonstrated ability to improve efficiency and quality of documentation processes.”
research	Researching, fact checking “learning about products and their nuances.”
style guides	Use or creation of style guides, publication standards, publication best practices, templates
domain expertise/experience – CS/IT	“Understanding of concepts related to information security, identity and access management, privileged access management, data loss prevention, and cybersecurity” “Understanding of IT security” “general cybersecurity experience” Specific experience—general technical in nature Endpoint security
domain expertise/experience - Other	Financial, privacy, gov’t, etc.
translating complex material	“translating and composing technical information into clear, readable documents to be used by technical and non-technical personnel.”
UX/UI	User experience, user interface & testing
visual rhetoric	“Excellent sense of design, workflow and content layout” formatting “layout skills”
Web design	
communication - SMEs	Work with technical teams Communicate with experts Interview analysts
writing – CS/IT	“experience required as a technical writer working within the information technology industry” “Cyber security/IT security professional writing experience.”
assurance	Audit, risk management, regulatory, compliance
standards/frameworks	NIST 800-series, FIPS, risk management

	frameworks
governance	Creating/maintaining policies, procedures, standards
meetings	Planning, note taking, leading, presenting “Experience preparing formal briefings and documenting critical discussion items, decisions, and task assignments from meetings”, presenting
graphics	“computer graphics” , graphic design
instructional design/training	Training, instructional design, training methodologies, learning principles, awareness program
writing - proposals	Writing proposals, understanding of proposal process, responding to bids
Agile	“experience with Agile/Scrum methodologies’
marketing	Marketing, SEO, sales collateral
analytics	Analytics, data science, data analysis, Web analytics
writing – Web	Blogging, wikis, online communities

Characteristics (soft skills) Codes

analytical	Analytical/critical/strategic thinking
collaboration	Collaboration/teamwork, remote/distributed teams, team environment
creativity	Creative, innovative, visionary
detail oriented	Obsessed with accuracy, attention to detail, quality
flexibility	Able to adapt/adjust, constantly changing environment, operate under pressure, dynamic environment, changing priorities, versatile, stress tolerance
independence/initiative	Proactive, assertive, take on challenges, proactive, self-starter, able to work alone, work without supervision
interpersonal	People skills, interpersonal skills, interface with people, team player, interact, works well with others, tactful, customer service, sense of humor
leadership	Managing others
learning	Willing to learn new skills, curious, intellectual, hunt down information
organization	
problem solving	Problem solving, troubleshooting, resourceful, quick decisions, ingenuity, judgment calls, not

	afraid to ask questions
time management	Time management, prioritizing projects, handle multiple projects, multitasking, deadlines, multitask, organize tasks
communication	Unspecified, oral/verbal/written Grasp of English
enthusiasm	Passionate, enthusiastic, positive
motivation	Results driven, focused, work ethic, productive
technology	Comfort with technology, able to learn new technology, apply technical skills in new situations, tech savvy , understand complex topics
integrity	Ethics, values, integrity, kindness, authenticity

Appendix B: Job Titles

Categorized as TC

- Technical Writer
- Technical Writer/Editor
- Technical Editor
- Assistant Proposal Writer
- Content Manager and Technical Writer
- Content Marketing Writer
- Content Writer
- Digital Strategist
- Instructional Designer
- Intern-Social Media
- IT Intern - Technical Writer
- Part-time Content Writer
- Plans and Policy Specialist
- Policy, Communications and Technical Writer
- Product Documentation Writer
- Senior Technical Marketing Writer
- Senior UX Writer
- Technical Editor - Shelter
- Technical Editor, Multimedia
- Technical Policy Writer
- Technical Writer (Documentation Specialist)

- Technical Writer/Graphic Designer
- Technical Writer/Publications Editor
- Technical Writer/Training Developer
- Technician Writer
- Web Content Editor
- Web Content Publisher

Categorized as CS (general)

- Cybersecurity Technical Writer
- Cyber Security Specialist / Technical Writer / Trainer
- Cyber Technical Writer & Editor
- Information Security Instructor
- InfoSec HowTo Writer
- Proposal Writer, IT Security
- Security Policy Technical Writer

Categorized as CS (specialized)

- CCBD Technology - Architecture - Technical Writer
- Cloud Security Technical Writer
- Cyber Policy & Awareness Manager
- Cybersecurity Standards Manager
- Cybersecurity Tech Policy Writer
- Information Assurance Specialist
- IT System Security Plan (SSP) Writer
- Network Operations Information Security Instructor

- Senior Content Developer, Cloud and IT Security
- Senior Technical Writer (Behavioral and Attack Analytics)
- System Security Engineer and Technical Writer
- Tech Editor / Writer (Cybersecurity Risk Management)
- Tech Writer, SaaS Security
- Threat Publications Part-Time Intern - Undergrad

Appendix C: Interview Responses

Response 1

1. **How long have you been a technical communicator in cybersecurity?**

    14 years.

2. **Did you start from the technical communication side or the cybersecurity side?**

    TC.

3. **What is your current title?**

    Information Security Office - Program Manager

4. **Please briefly discuss your current role and duties.**

    Build a security awareness/phishing training program; draft policy, procedures, and supporting documentation; and manage projects/programs.

5. **What projects and/or deliverables do you work on/produce most often?**

    - Policy and procedure
    - Training materials (awareness and phishing)
    - Project planning/strategy
    - Social media
    - Web content
    - UX/UI

6. **Can you discuss how you ended up in cybersecurity?**

    While working at a university, the participant was brought on by the Information Security Officer to handle communications around a cybersecurity incident. From there, the participant was formally brought into the Information Security Office to communicate with end users and has since shifted into a program/project manager role.

7. **Did you have any education, training, or certifications in cybersecurity prior to entering the field? If so, what was it?**

   No.

8. **While in your current position, have you had any cybersecurity-specific education or training? If so, please describe.**

   Earned CISSP certification and has received informal training through Educause participation.

9. **Was the position contingent on that training?**

   No.

10. **Do you plan to continue cybersecurity-specific education and training?**

    Nothing formal—conference attendance and similar.

11. **Is ongoing cybersecurity education required for your role?**

    No.

12. **Do you think that cybersecurity-specific education or training has been beneficial to your role?**

    "It made me feel much better in terms of knowing I understood the subject matter better. Also in terms of being able to talk with technical folks to understand what they're talking about--making sure that I really have a good grasp of what they're telling me."

“Probably the biggest thing which is a direct result of any of that training is looking at things from a risk management framework. Because we're not able to eliminate risk--it's always about managing risk and making decisions based on the risk profile. Probability, impact, and making decisions based on that.”

13. Please briefly discuss your education and training outside of cybersecurity.

- Entered TC as a doctoral student in early modern European history (did not complete)
- Received a graduate-level advanced technical writing certificate

14. What cybersecurity-specific skills and/or tools do you use most often?

- N/A

15. What advice do you have for somebody wanting to become a technical communicator in cybersecurity?

“Learning that vocabulary. Getting a baseline understanding. It helps tremendously if you've had any IT background at all…. It gives vendors and professionals a shared vocabulary. So learning the vocabulary is important.”

Once you have learned the vocabulary, practice using it, such as through white papers or ghost writing.

16. Do you have any other comments that you’d like to make?

The TC skill set can be easily applied to CS “because our biggest issue is still people, and people understanding what they need to be careful of and training them to recognize things, and know how to deal with them.”

“It's such a huge growth field for us. It's a great spot. I think it's a great area for TC to go into…. It's a vibrant, growing, rich field… the pay's good…. It's growing more and more complex, so there's more and more work to do. It's a growth field, and I think that's important.”

Response 2

1. **How long have you been a technical communicator in cybersecurity?**

   5-10 years, cumulative across several full-time or contract positions.

2. **Did you start from the technical communication side or the cybersecurity side?**

   TC.

3. **What is your current title?**

   Governance Risk and Compliance IT Security Policy & Procedure Writer (most recent)

4. **Please briefly discuss your current role and duties.**

   Between roles currently, but previous positions were mostly what you’d think of as traditional “standard fare,” e.g., technical writing, working with SMEs, project planning.

5. **What projects and/or deliverables do you work on/produce most often?**

   - Policies, standards, procedures, guidelines
   - Templates
   - Installation manuals, user guide, troubleshooting guides
   - Prototypes/dummy docs
   - SOPs

6. **Can you discuss how you ended up in cybersecurity?**

After being laid off following several years in various TC positions, the participant was contacted by a recruiter looking for somebody with experience in policies and procedures to work in the information security department of a large supermarket chain.

7. **Did you have any education, training, or certifications in cybersecurity prior to entering the field? If so, what was it?**

No.

8. **While in your current position, have you had any cybersecurity-specific education or training? If so, please describe.**

Cisco Certified Network Associate from a previous position.

9. **Was the position contingent on that training?**

No.

10. **Do you plan to continue cybersecurity-specific education and training?**

Currently working toward CISSP. Considering PMP and CISA. Any one of those certifications--you don't really need them for IT security.

11. **Is ongoing cybersecurity education required for your role?**

N/A

12. **Do you think that cybersecurity-specific education or training has been beneficial to your role?**

“All of a sudden the engineers were a lot more willing to talk to me. Because before they thought I was just one of those "English teacher" type technical writers who didn't have a clue about technology, but was pretty good with knowing where the apostrophes and commas are supposed to go. But by having a CCNA, all of a sudden I could walk in and talk to the engineers, and they were like, 'Wow, you're one of us!'"

13. **Please briefly discuss your education and training outside of cybersecurity.**

Biology degree; management of technical documentation certification; Agile bootcamp.

14. **What cybersecurity-specific skills and/or tools do you use most often?**

Passwords, firewalls, VPNs.

15. **What advice do you have for somebody wanting to become a technical communicator in cybersecurity?**

"First of all, just be darn good at English grammar, spelling--eagle eyes for finding typos--organization, syntax, that type of thing."

"[Have a] good command of technical vocabulary--it doesn't freak you out to see highly technical terminology…. If you know the lingo... when you see that on a job posting, that is a clue that if you can write about it or do research on it, you'll be knowledgeable about it when you apply for the job. Sometimes you gotta jump in the pool and start swimming before you learn what swimming is--you can't just read about it."

"For anyone wanting to get into technical writing, I'd say do freelance writing on the side…. There are so many weird things you can write about. Write about a topic and send it to a trade journal, and now you have published work to put in your portfolio that you can show people…. So I'd advise anyone wanting to get into IT security or any other topic--just write articles about it…. And then get it published on LinkedIn."

Attend local CS conferences, such as RSA or SANS, and network. Also attend TC conferences.

Become familiar with regulations and standards such as ISO27000, NIST SP 800-53, FISMA, HIPAA, PCI DSS, and GDPR.

If possible get clearances through your current job.

16. Do you have any other comments that you'd like to make?

"If you're interested in any field--even if it's not cybersecurity--there is a need for cybersecurity. [Everyone]] needs IT security. So if you can go to conferences that don't involve IT security, and you pass out a business card that says that you can do IT security, you might get some raised eyebrows."

"And if you look at job openings, it's obvious that the people asking for tech writers do not have a clue what a tech writer is…. They have no clue what they need; they just have a bit of pain, but somebody told them they need a tech writer--but they have no clue what a tech writer does."

"But in IT security, there's a lot less competition because tech writers haven't figured out that this area is even here."

Response 3

1. **How long have you been a technical communicator in cybersecurity?**

   More than 25 years.

2. **Did you start from the technical communication side or the cybersecurity side?**

   Started from the technical side, then into technical communication, and then into CS.

3. **What is your current title?**

   Senior Cybersecurity Analyst, Governance, Risk, and Compliance (GRC)

4. **Please briefly discuss your current role and duties.**

Manage the GRC posture of large and complex systems used for training and simulations.

5. **What projects and/or deliverables do you work on/produce most often?**

- Security documentation
- System security plans
- Security design documentation
- Interconnection plans and agreements
- Incident response plans
- Disaster recovery plans
- Plans of action & milestones
- Test plans
- Reports

6. **Can you discuss how you ended up in cybersecurity?**

There was a need: Systems that are accredited by the DoD are dependent upon good documentation. And "…the money is pretty danged good."

"I have always been interested in technology and my tendency is to want to read about things I am interested in. And, years ago, when I looked for things to read about technology, I either found NOTHING – or I was appalled by what I read…. So I stepped in to write documentation on a database system that I was the accidental SME on, and then they needed a configuration management plan, and well, the rest is history."

7. **Did you have any education, training, or certifications in cybersecurity prior to entering the field? If so, what was it?**

Yes.

8. **While in your current position, have you had any cybersecurity-specific education or training? If so, please describe.**

   Yes, certification with ongoing training requirements.

9. **Was the position contingent on that training?**

   Not at the time.

10. **Do you plan to continue cybersecurity-specific education and training?**

    Yes.

11. **Is ongoing cybersecurity education required for your role?**

    CISSP was required.

12. **Do you think that cybersecurity-specific education or training has been beneficial to your role?**

    Yes, to keep up with trends and emerging requirements.

13. **Please briefly discuss your education and training outside of cybersecurity.**

    - Bachelor’s in Information systems with an emphasis on databases and the relational model
    - Master’s degree in library and information science with an emphasis on federal information policy.

14. **What cybersecurity-specific skills and/or tools do you use most often?**

    - Scanning tools, like (Nessus)
    - SCAP (a protocol for automating server hardening)

- WireShark (for network traffic and DoD packet analyzers)

15. **What advice do you have for somebody wanting to become a technical communicator in cybersecurity?**

"Gain subject matter expertise and just volunteer. Good writing and editing skills have been welcome in every single group I have ever worked around! An entry level certification in cybersecurity also helps a lot."

16. **Do you have any other comments that you'd like to make?**

No.

Response 4

1. **How long have you been a technical communicator in cybersecurity?**

   Almost 10 years

2. **Did you start from the technical communication side or the cybersecurity side?**

   TC

3. **What is your current title?**

   Knowledge Base Manager

4. **Please briefly discuss your current role and duties.**

   - Manage/coach team of three technical writers
   - Manage KB content (online support portal, help content, style guides) and KB tools (maintenance, updates/patching, troubleshooting), CMS/authoring tools
   - Updates to content: adding, clarifying, editing, correcting based on SME feedback
   - Work with business partners

- Ensure content is complete and accurate for new or updated products
- Quality reviews for content
- Project/program management

5. **What projects and/or deliverables do you work on/produce most often?**

   - Style guides
   - Manuals/user guides
   - KB content

6. **Can you discuss how you ended up in cybersecurity?**

   Referred by friend.

7. **Did you have any education, training, or certifications in cybersecurity prior to entering the field? If so, what was it?**

   No.

8. **While in your current position, have you had any cybersecurity-specific education or training? If so, please describe.**

   No.

9. **Was the position contingent on that training?**

   N/A

10. **Do you plan to continue cybersecurity-specific education and training?**

    No plans.

11. **Is ongoing cybersecurity education required for your role?**

No. Domain-specific (rather than cybersecurity) training is recommended based on roles. (E.g., Training specific to the systems you are documenting.)

12. Do you think that cybersecurity-specific education or training has been beneficial to your role?

N/A

13. Please briefly discuss your education and training outside of cybersecurity.

- Prior to employment: Bachelor's in English
- During employment: Master's in TC (UX focus)
- During employment: PhD in TC in progress (encouraged by manager)
- Master's and PhD beneficial for moving into management role; probably would not have been useful if stayed in non-management role

14. What cybersecurity-specific skills and/or tools do you use most often?

Ransomware

15. What advice do you have for somebody wanting to become a technical communicator in cybersecurity?

Computer science or domain-specific education might help get your foot in the door, but education and experience with writing and editing (communicating complex information about cybersecurity topics to many different audiences) is going to be more useful as a technical writer.

Need to be able to understand new technologies quickly an enjoy working with new technologies. "Being able to learn a new piece of software very quickly is important. You can tell who has a natural knack for it, or an interest in learning these types of things."

Bachelor’s degree in anything shows somebody who can finish what they start and handle responsibilities.

Education and experience with writing and editing is going to help more than security certifications. Having more experience writing very complex information about cybersecurity topics or editing for varied audiences is a little more beneficial than just having domain knowledge in cybersecurity.

16. **Do you have any other comments that you’d like to make?**

“I think that anybody who is a technical writer and who wanted to focus more on software or has some domain knowledge, then you would be able to get a job in cybersecurity for sure.”

“And it's a really exciting job to have, and it just better than just having a tech writing job at a company that's makes dialysis equipment or something--just boring. It's really exciting every day. And I feel really lucky that the company grew a lot during that time too, so I've been really fortunate.”

“We have all these jobs open and it's interesting that you can't get candidates that really fill what you need. So trying to find somebody that has an education in technical writing in some way--like writing for technical audiences--doesn't have to have a technical writing degree even. And then have some interest and knowledge in working with software or technology. It doesn't seem like a lot, but finding those two things is actually more difficult than I expected.”

Response 5

1. **How long have you been a technical communicator in cybersecurity?**

Since 2015.

2. **Did you start from the technical communication side or the cybersecurity side?**

   Originally a journalist for computer magazines and became a technical writer.

3. **What is your current title?**

   Independent Security Officer

4. **Please briefly discuss your current role and duties.**

   - Governance and oversight
   - Oversee penetration testing vendors
   - Follow up on testing

5. **What projects and/or deliverables do you work on/produce most often?**

   - Test reports
   - Memos to upper management
   - PowerPoint slides

6. **Can you discuss how you ended up in cybersecurity?**

Temporarily left TC to work for a nonprofit but was referred by a friend for a position as a CS journalist. From there, applied and got more traditional TC position in CS via LinkedIn.

7. **Did you have any education, training, or certifications in cybersecurity prior to entering the field? If so, what was it?**

   No.

8. **While in your current position, have you had any cybersecurity-specific education or training? If so, please describe.**

Prior company: SANS 401 (GIAC-GSEC)

9. **Current company: CISSP**

10. **Was the position contingent on that training?**

“The job was contingent on CISSP, no question. It was a requirement. And it actually does help during the day to day.”

11. **Do you plan to continue cybersecurity-specific education and training?**

Considering:

- AWS Sysadmin
- CEH
- CISA

12. **Is ongoing cybersecurity education required for your role?**

No.

13. **Do you think that cybersecurity-specific education or training has been beneficial to your role?**

“A lot of the more technical stuff from the SANS401 that I wouldn't use in a primarily technical communicator role, I'm actually using now…. I can have a better vantage point to better understand what the [SMEs] are saying and whether they're being thorough and giving a good analysis… So it does get you an 'in' there…. It actually helps to be conversant and all these things.”

They don't guarantee anything, but they do help marketability.

14. **Please briefly discuss your education and training outside of cybersecurity.**

Bachelors in journalism.

15. What cybersecurity-specific skills and/or tools do you use most often?

- Managed security service providers (MSSP)
- Splunk
- Tableau
- Vulnerability management

16. What advice do you have for somebody wanting to become a technical communicator in cybersecurity?

"I think that there's a lot of self-education that people can do. You just have to start reading the best sources on a consistent basis and develop that. They should probably find one thing that they want to focus on--that they understand well…. If there's some breach that caught their imagination or horrified them."

"[If you're interested in AWS], look at AWS security and get a free AWS account and just play around with some of those things. [If you're interested in penetration testing], get the Metasploit book, download Metasploit, and get some fluency with what these tools look like…. and suddenly the light bulb will go off and they'll start to go in that direction."

"And then they have to try writing something. You'll need writing samples. A blog, even if nobody reads it can shows you know what you're talking about and could help you get through the door."

Example reading to get started:

- *SC Magazine*
- *Dark Reading*

- *Security Week*
- *Krebs on Security*
- *Verizon Data Breach Report*

17. Do you have any other comments that you'd like to make?

"This is a hands-on security job… that puts a premium on communication skills for cultural and organizational reasons. I still think that's my value add: I can write fast, and I can do a decent job. In this kind of role—and this may be underestimated because it's more of a bureaucratic organizational skill—where just writing the right email to the right person at the right time in the right way to get something done or get their attention actually makes a difference."