Taran Pearce

Cybersecurity LAS Project

Cybersecurity and Technical Communications and Information Design

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks, and technologies. - https://www.itgovernance.co.uk/what-is-cybersecurity

This report covers the primary issues and competencies of cybersecurity in relation to the TCID program available at the University of Colorado in Colorado Springs. After covering the core skills and problems to be solved, the paper dives into several career options that may become available to those graduating the TCID program, including one advanced position that one can work towards once in the field.

What doors can cybersecurity open for technical writing majors?

Issues in Cybersecurity That Are Important to Technical Writers

Complexity

One of the primary issues of Cybersecurity is the complexity of the content. Rsisecurity states that "Not everyone can grasp complex ideas, particularly as they relate to information technology and cybersecurity." In the same way that technical writers are necessary for any other job with complex information that needs to be understood by a wider audience, cybersecurity demonstrates a need for breaking down these complex information technology issues and redistributing the information in digestible ways for the novice coworker. Due to the complex nature of designing informative texts around computer science issues, technical writers focus heavily on simplifying this information for the consumption of other workers.

Social Engineering

Along with complexity come the topics that writers may need to discuss, such as social engineering. Technical writing proficiencies developed throughout the TCID degree plan focus on this competency in particular, and in turn, open numerous doors to proceed into cybersecurity. According to Maryville.edu, social engineering is a term that refers to all of the different methods hackers engage in to steal important information. Hackers will utilize "tactics designed to trick individuals into giving out sensitive or confidential information" through "emails designed to look like they come from a legitimate source, such as a business, bank, or a government agency." While plenty of other methods of exposing the business's network to malware exist, technical writers are primarily concerned with the usage of emails in malware. Technical writers with a cybersecurity

focus look to guide and prevent their coworkers from mistakenly interacting with hackers implementing such methods in order to better secure the network the business runs on.

Cybersecurity technical writers also:

- Write manuals on how to prevent cyberattacks through social engineering (for example, informing coworkers of the danger of clicking links in emails)
- Create manuals on how to recover from cyberattacks through social engineering
- Inform coworkers through written guidelines on what interactions to avoid and who to go to when information is suspected as malware
- Collect Data on social engineering methods to better prepare the company for future attacks

These are a few overarching ways technical writers get involved in helping their company prevent social engineering from malicious individuals.

Defense

Just like a real battle, cybersecurity focused writing tends towards either offense or defense. According to the bachelor's in cybersecurity program for Maryville university, several tracks are available for those looking to get involved. Three such tracks are the defensive track, offensive track, and the general track. Technical communications tend to lie in the defensive sector, as they are more concerned with the protection of information and guiding their company in these matters. On the contrary, an example of offensive testing where a technical writer might get involved is the company hiring individuals to hack their systems and explain the vulnerabilities. A technical writer may collect this data and utilize it in guidelines and procedures for the company.

Main Competencies

The competencies of those involved in cybersecurity have been thoroughly researched and evaluated by the United States Department of Labor. Figure 1 displays the soft skills required of those in the cybersecurity industry (CareerOneStop). Many of the same core competencies of technical writing are also present in the Department of Labor's set of required skills.

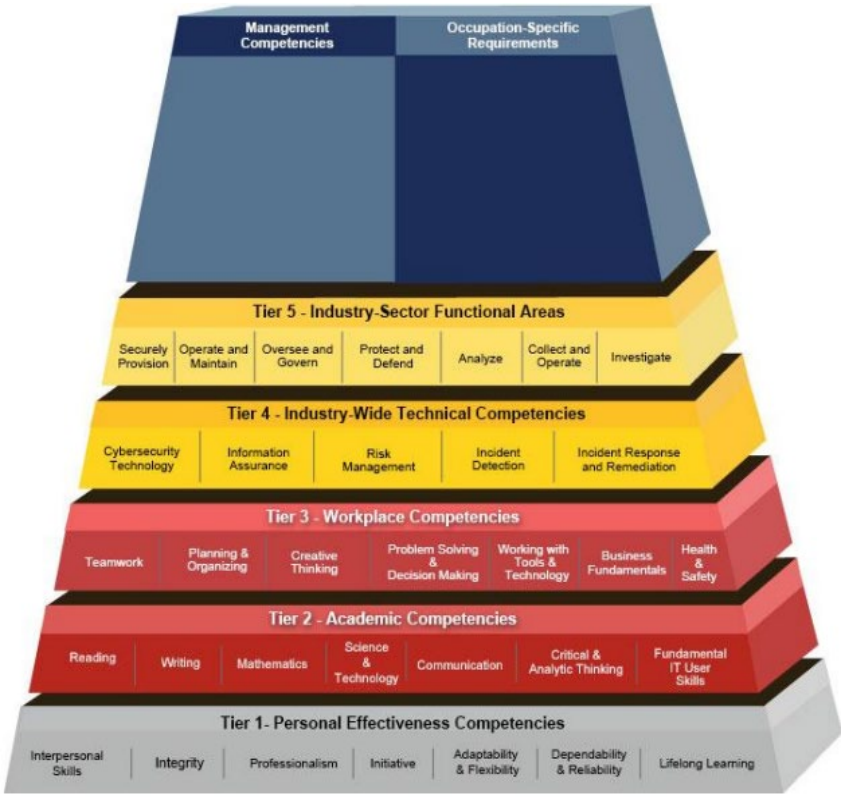

Figure 1: Cybersecurity Competencies CareerOneStop

Notable specific skills include:

- *Adaptability and Flexibility*: This skill is required in technical communication, as learning modern technologies becomes a daily activity.
- *People Skills and Teamwork*: Though this skill is not explicitly labeled collaboration, it holds the same meaning, as teamwork is critical to success.
- *Writing and Communication*: The ability to write well carries over with many fields and cybersecurity is no exception.
- *Planning and Organizing*: The ability to manage deadlines and projects is an easily transferrable skill from technical writing.

How A Technical Writer May Obtain Other Cybersecurity Competencies

It is quite reasonable and useful for a technical communication and information design major to transfer their skills into cybersecurity. If a technical writer is looking to get into cybersecurity, they would be well advised to further their education in computer science (or at least the terminology) to better understand the content they are writing around. For example, a class involving a brief overview of the many different programming languages and their relationship to businesses would be an excellent section Figure 1 in a TCID/computer science course.

Career Paths in Cybersecurity with A Technical Communications focus

Cybersecurity Technical Writer

Median salary of $70,000

The cybersecurity technical writer is the primary role that a technical communication and information design graduate would look for. This career path is directly related to the TCID degree (documentation creation, updating information, interviewing subject matter experts) and provides a great entry point for other positions in the cybersecurity industry.

What do they do?

Cybersecurity technical writers create security plans including preparation for cyber-attacks, responses to cyber-attacks, and recovery from cyber-attacks. These writers will also update information in the corporation's systems to better reflect modern methods of protecting important information.

What does entry-level experience look like?

- Many companies prefer prior experience creating specifically cybersecurity documentation, although, this may be offset by previous experience creating documents that can be compared to items such as security plans, end user documentation, or manuals/guides.
- A bachelor's degree or equivalent experience is required in nearly every single entry-level cybersecurity technical writer job posting.
- Secret or top-secret clearance is usually necessary, but companies or contractors will help employees get clearance.
- The ability to interview subject matter experts on information that is relevant to the creation or updating of information for the company or industry for which one is working.

Junior Information Security Analyst

Median Salary of $53,138

This role is an entry-level role that performs basic analysis over security processes and procedures to identify and prevent cyber threats.

What do they do?

According to Ziprecruiter, junior information security analysts "duties may include establishing threat plans and protocols, maintaining data, monitoring security network access, performing tests and risk analysis, reviewing security alerts and taking steps to protect the information, updating and maintaining a firewall, and recommending security tools and countermeasures to your superiors."

What does entry-level experience look like?

- A bachelor's or equivalent experience is usually required, but some companies may offer extensive training.
- Previous experience analyzing cyberthreats a plus.
- Previous experience writing documentation related to cybersecurity a plus.

Blue Team Member

Median Salary of $83,000

This is a specified role revolving around the defense of a company in relation to cybersecurity. Many technical writing competencies are directly relevant to the major job functions of a blue team member.

What do they do?

According to Purplesec, blue team members "establish security measures around key assets of an organization. They start their defensive plan by identifying the critical assets, document the importance of these assets to the business and what impact the absence of these assets will have." Blue team members will also "perform risk assessments by identifying threats against each asset and the weaknesses these threats can exploit."

What does entry-level experience look like?

This is a position that may require a bit more time and involvement directly with cyber security, as such, it is preferred by most companies for candidates to have some experience as a junior information security analyst first.

- A bachelor's or equivalent experience is required for candidates in every job posting.
- One should have previous experience with analyzing cyber-threats.
- Previous programming (C basic, C++, C#, Java, etc.) experience is a plus.

Take-aways for TCID Majors

While obvious, many job opportunities would hope for some level of experience with cybersecurity before applying; however, the actual qualifications for several jobs are quite easily attainable with even just a bachelor's degree in technical communication. A course specifically introducing those in the Bachelor of Arts section of the university to cybersecurity may be all that is necessary for someone in the TCID program to develop an interest. Entry-level experience is quite inclusive for two of the major roles, and both cybersecurity technical writers and junior information security analysts will receive extensive training before they are left on their own. Blue team member positions tend to be more advanced, but a showcase of a pathway one could go down is important for those looking to get into the field.

References

https://blog.rsisecurity.com/what-makes-a-great-cybersecurity-technical-writer/

https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx

https://essentialdata.com/the-five-ws-cybersecurity-technical-writer/

https://www.indeed.com/

https://www.itgovernance.co.uk/what-is-cybersecurity

https://online.maryville.edu/blog/cybersecurity-issues/

https://purplesec.us/red-team-vs-blue-team-cyber-security/#Blue

https://www.stu.edu/news/top-3-careers-in-cyber-security/

https://www.ziprecruiter.com/

https://www.ziprecruiter.com/e/What-Does-a-Junior-Cyber-Security-Analyst-Do