An Analysis of the Entry-Level Cybersecurity Engineer Position for CGI

Gregory S. Oehm

School of Cybersecurity, Old Dominion University

IDS 493: Electronic Portfolio Project

Prof. Sherron Gordon-Phan

February 9, 2026

Abstract

This paper aims to determine what skills and expectations are sought for the given entry-level job of a cybersecurity engineer for CGI, and whether or not the position would be suitable for me, given my skills, expectations, and needs. To do so, the advertisement is examined closely in an attempt to reveal the most crucial skills needed to work in the role, with care taken to analyze all parts of the listing. The company's overall environment and culture are also investigated. These skills and abilities are then compared to my own. Given that a large majority of the requirements that are either laid out or implicitly demonstrated can be met by me, due to the university courses I have taken, it can be determined that I hold the proper skills to fill this position, and perhaps other entry-level positions that are similar. While this exact position would not work for my purposes, a similar role in a different company would be satisfactory.

An Analysis of the Entry-Level Cybersecurity Engineer Position for CGI

The job market in today's world can be rather troublesome, for many individuals. In the world of cybersecurity, however, there are quite an abundance of available jobs, with professionals in the field being in high demand. One company recently looking to add more employees to their staff is CGI, a technical consulting organization. Among their job postings is one for an entry-level position as a cybersecurity engineer. A close examination of the responsibilities and required skills of the role, alongside other related information, indicates that it is quite suitable for those that wish to obtain a job in the field of cybersecurity for the first time, such as myself.

Position Responsibilities

The role of an entry-level cybersecurity engineer within CGI seems to carry several important responsibilities, as laid out in its job advertisement. Chief among these seems to be helping to implement technical cybersecurity controls within client organizations which, as stated in the posting, include "vulnerability scanners, endpoint protection tools, firewall, VPN, and network access control" technologies (CGI, n.d.). Each of the controls listed here, among others, can be crucial for helping patch vulnerabilities and protect against threats, with each client organization likely needing different controls based on their resources, exposure to threats, risk appetite, and the overall context the organization finds itself in. As such, utilizing a specialist who is familiar with the installation of these technologies can help make them more secure. Working to maintain these tools, as well as documentation and records of the controls and architecture already in place is also listed as a top responsibility (CGI, n.d.). As a consulting organization for government agencies, it seems natural that those in the company would be expected to return to the same agencies periodically. Keeping records can allow

misconfigurations or other issues in a system or network to be more easily identified, help ensure changes do not bring with them unintended harm, and allow for faster recovery in the event of damage. Further, the job advertisement suggests that the person in this position will be responsible for helping transition certain components of agencies onto cloud platforms, while developing secure communication paths (CGI, n.d.). Working with cloud technologies has become increasingly common in recent years due to the trend of decentralized computing, with many organizations favoring subscription models rather than purchasing expensive technical components for their own use. These two responsibilities seem to go hand in hand, as secure communication paths between agencies and resources would be necessary to most effectively make use of cloud technologies in a secure manner, given that sensitive data could otherwise be transmitted over insecure channels. In addition, the cybersecurity engineer is described as needing to help agencies carry out monitoring capabilities (CGI, n.d.). Though it is not stated whether the cybersecurity engineer would actually help monitor against threats or simply assist the agency in creating a program to continually look for cyber threats themselves, the latter seems more likely, as a program largely supported by the agency itself would be able to identify and respond to attacks in a more consistent manner, while reducing the exposure of sensitive information to outsiders.

Required and Beneficial Skills, and What They Reflect

Several kinds of skills and qualifications would be needed for a job such as this, many of which are described in the job advertisement itself. First, the cybersecurity engineer must be able to apply cybersecurity skills to “approach difficult and narrowly defined technical problems to arrive at automated solutions,” hinting that critical thinking and problem solving abilities, in conjunction with a strong understanding of cybersecurity, would be needed for this job (CGI,

n.d.). A bachelor's degree is also stated as a requirement, further indicating that a large library of knowledge would be key to solving many of the problems that the engineer might face in creating and implementing a strong security architecture (CGI, n.d.). "Experience with scripting languages," or programming languages, is also needed (CGI, n.d.). This helps demonstrate that theoretical knowledge alone is insufficient. The ability to translate this knowledge into actual change within an agency would thus be key, to at least some degree. Both the ability to work with others and strong communication skills are listed as requirements, as well (CGI, n.d.). This reinforces the idea that the cybersecurity engineer will be working closely with others, both in their own workplace and in the agencies which they will visit, in order to create the best outcomes for client agencies. Being able to communicate what the goals of the architecture should be, and how to best reach these goals, are seemingly crucial. Another surprisingly insightful requirement listed is a "phenomenal attitude and hunger for learning" (CGI, n.d.). While, at a first glance, this may seem to be another fairly standard requirement, it can actually indicate quite a lot about the job and cybersecurity as a field. New kinds of vulnerabilities are found every single day, and new threats can appear around the globe just as frequently. Being able to stay abreast of these changes, and the techniques developed to mitigate their impact on organizations, is a key skill for nearly all cybersecurity professionals. Keeping a calm mind and attitude can be similarly important, given the high stress situations that might arise during an attack or if a key system otherwise fails. So, while a pleasant attitude and the ability to learn are certainly helpful across essentially all fields, they can be particularly critical for cybersecurity professionals, including cybersecurity engineers. Though it is not directly listed in the qualifications section, a familiarity with cloud environments would also likely be necessary to best provide assistance to clients when moving services to the cloud, perhaps indicating that this

responsibility will be shared among numerous people within the organization, which would not be far fetched given that the job advertised is only entry-level, or that their cloud implementation is not overly technical. Further, another soft skill that seems critical for this position, and one that is not described directly, is a high degree of flexibility. Organizations can change their goals rather quickly, in some circumstances, and the best controls might vary from agency to agency. While high level concepts and objectives will likely be fairly consistent across each organization, being able to switch from one approach to another, without being locked into a single methodology, can allow for better results across a wide variety of potential clients. The notion that flexibility could be crucial for the position is supported by an early descriptive paragraph on the page, as well, detailing the role as "exciting" (CGI, n.d.). It states that "one moment you could be developing a cybersecurity solution" and "the next you could be working with your manager to map out your career goals," quickly followed by "addressing flagged vulnerabilities" (CGI, n.d.). The job itself is also described as "hybrid," meaning that it has both in person and remote elements (CGI, n.d.). Clearly, new tasks will appear routinely, with flexibility remaining important throughout in order to prioritize and keep up with constantly shifting objectives and the work environment as a whole. Overall, though, the most crucial skills would appear to be a large overall body of cybersecurity knowledge and familiarity with the discipline, as well as strong interpersonal and communication skills. The former plays a role in the top three skills listed, and both play at least some role in most responsibilities or topics discussed throughout the advertisement. Other forms of education, experience, and training that support and provide evidence of this knowledge, while not listed, would likely be valued as well. This might include certifications like CompTIA's Security+ and ISC2's CC for general cybersecurity competency, and GIAC's GCIH for incident response, among many others.

Other Notable Features of the Position and Company

Quite a bit can be inferred about the job and CGI itself beyond this. Clearly, the position has been delineated as "entry level" (CGI, n.d.). Despite this, it is important to recognize that this is truly the case. Many employers will list a job as entry-level, but will require excessive experience or education that most entry-level workers could not realistically meet. In this case, however, the job's requirements are actually minimal. Only a conservative amount of academic experience is listed as necessary here, with no part of the posting indicating that prior work experience in the field is critical to being given the position (CGI, n.d.). So, while the individual in this role will still have an important position, assisting in seemingly important and meaningful work for clients, they would not be overly authoritative in the organization as a whole. CGI, as a company, has a separate page dedicated to the culture of the organization, which can shed insight into what working for the company might be like, as well. The company appears to value the opinions of employees more than many other organizations. The organization enables employees to become shareholders of CGI, while regularly surveying them about their satisfaction and feelings towards the company, giving them a voice and at least a small amount of practical influence (Godin, n.d.). The organization as a whole also seems dedicated to providing quality services to their clients, stating that "delivering the best services and solutions to fully satisfy client objectives," among other commitments, are the core "mission" of the organization and those who work within it (Godin, n.d.). The company as a whole seems quite professional and goal-oriented as a result, while retaining a great deal of consideration for its own employees.

How Personal Skills Apply to the Role

Many of the courses I have taken have granted me the required skills to work in a position such as this. The ability to make scripts is, as discussed, needed for this role. The

programming course I have taken at Old Dominion University has provided me with the foundational skills in this regard, giving me knowledge of, and experience with, the Python programming language, which could be built upon in this role. My communication skills in the realm of cybersecurity have also been supported by human factor and cybersecurity policy courses, potentially allowing for more effective interactions with the clients CGI works with. The listing's indication that working with an "agency's architecture and configurations" will be a large component of the job speaks to my understanding, as well, at least to some degree (CGI, n.d.). The networking and networking-related courses I have taken have given me a good understanding of how new tools and controls fit into larger and preexisting network structures and how new networks and subnetworks can best be implemented. While I believe I hold most of the skills necessary to fulfill this position, this does not mean improvement is unneeded or undesirable. I have yet to actually obtain my bachelor's degree in cybersecurity, though this issue should be resolved within a relatively short period of time. In addition, I would likely benefit from more experience in actually building networks and implementing and configuring network technology in the real world, rather than simply coming up with theoretical plans.

Motivating Factors and Other Thoughts About the Position

Several kinds of valuable benefits are provided alongside the role, of course, providing compensation for one's skills and the challenges they are likely to face when working in this position. The job's salary and benefits are naturally an important consideration. The salary range provided in this case starts at $74,600 and ends at $130,500 (CGI, n.d.). This seems to be a very suitable salary, especially for an entry-level position, with it being higher than the salary of many individuals in the United States. Cybersecurity is a growing field, faced with a significant shortage of workers, which may have contributed to this position's comparatively high salary.

Also included are “comprehensive insurance options” and parental leave, along with “wellness” and “well-being” programs which, while vague, indicate that more than just the base salary are offered to employees (CGI, n.d.). The primary factor in determining which jobs are appropriate for me, however, would be whether I can gain appropriate experience and advance my career while working in a given position, moving from being someone with just a degree and certifications to someone who also possesses a repertoire of practical cybersecurity abilities. Also critical is the capability to foster the desirable employability skills needed for future career advancement, that might not be obtainable in a purely academic setting, and which many individuals may be lacking otherwise (Harris & Clayton, 2018). As a result of the high demand for cybersecurity professionals, career growth in this field is arguably even more consequential as a result. Even beyond direct financial considerations, the advertisement is highly encouraging in this regard. “Learning opportunities and tuition assistance” are also included among the listed benefits, indicating that career growth and further education would be a valuable byproduct of employment at CGI (CGI, n.d.). The position is also entry-level, so it seems as though the expectations placed on the individual in this position, while not light, are also not unreasonably high. The site’s presentation, overall, does not indicate that a great deal of experience would be necessary, with it instead highlighting “opportunities to deepen your skills and broaden your horizons,” a valuable feature for someone such as myself (CGI, n.d.). Given the strong focus on collaboration described throughout the posting, it seems as though the cybersecurity engineer is to be matched with a group of cybersecurity professionals. This opens up the opportunity to grow one’s skills and advance their career by learning from others. Having to solve practical problems in cybersecurity would perhaps be difficult for the first time, even in an entry-level position such as this, with the individual in this position needing to implement a wide variety of tools and

technologies, some of which may be unfamiliar, in a wide variety of contexts. Even so, I do possess the appropriate skills to find these solutions, and would seemingly be supported in this case by other professionals. As such, any challenges faced in this position would seem to be by no means insurmountable, with the job serving as an opportunity to gain valuable real-world experience and connections. While I, of course, could not accept this position at the current time, as I have not yet finished my education, I would be more than willing to apply for a similar or identical position in the near future.

Concluding Thoughts

The job of an entry-level cybersecurity engineer at CGI seems quite compelling. The responsibilities laid out for the position appear quite engaging, in particular. Working to plan out, implement, and maintain technical controls for others will require applying cybersecurity skills and concepts to meet the needs of a variety of client organizations. Continued work with the same organizations, in order to help them monitor potential cyber threats and make use of new developments within their facilities, could allow the engineer to witness a large amount of progress over time. Several critical skills would be required in order to carry out these duties, including a deep technical knowledge about cybersecurity tools, resources, and techniques, being able to effectively communicate and negotiate one's approach with clients and other professionals, and the ability to solve problems efficiently and quickly while under pressure. Thankfully, I feel as though my academic career has sufficiently prepared me for most or all of these requirements. My future endeavors, such as in a job like this, would hopefully allow me to continue to grow and refine these skills. The company and work environment laid out in the advertisement itself, from what information is available, seem to be a good fit for someone entering the field of cybersecurity for the first time, such as myself. Especially compelling is the

promise of valuable experience and career advancement later on. Though this exact position may be inappropriate for me at the current time, examining the requirements for it and similar positions can help indicate where my training and education has been successful, and in what ways future improvements can best be accomplished.

References

CGI. (n.d.). *Cyber security engineer – Entry level.* theFreshDev. Retrieved February 8, 2026, from https://www.thefreshdev.com/job/cyber-security-engineer-entry-level-cgi-2944

Godin, S. (n.d.). The CGI culture. CGI. Retrieved February 8, 2026, from https://www.cgi.com/en/media/brochure/cgi-culture

Harris, R., & Clayton, B. (2018). Editorial: The importance of skills – But which skills? I*nternational Journal of Training Research, 16*(3), 195–199. https://doi.org/10.1080/14480220.2018.1576330