1. Knowledge of the techniques of the cybersecurity discipline, including encryption, access control, physicals security, training, threat analysis, and authentication.

When it comes to techniques in the cybersecurity disciplines it is important to remember at a very high level the CIA security triad of confidentiality, integrity, and availability. Keeping in mind how one can effect the other is imperative to producing and maintaining a good security posture. Another technique is to have a layered security approach. Having multiple layers of security can reduce the chance of a single point of failure, but can also reduce availability as mentioned in the CIA triad above.

Throughout my studies I have learned and applied a wealth of knowledge about encryption such as using John the Ripper on Kali Linux to crack MD5SUM hashes via brute force and dictionary attacks, this was done in my undergrad and CEHv9 training. I have also written a program in Java using AES and is publicly available on my [github](https://github.com/webberic92/EncryptionExample). One of my huge passions is blockchain technology which is centered around encryption and hashing. I have GPU and ASIC miners designed to solve Bitcoins hashing algorithm which is based on double SHA-256, along with other blockchain mining and Proof – of – Stake projects.

Access-control is another technique I have dealt with not only in my studies through my CEHv9 and TestOut Security Pro Certification, but is also something I have applied in the real world. In my previous vocation as a VOIP administrator we would have to create ACL to allow or block certain users from having access. Keeping in mind that policies and procedures should be in place to only allow what users need.

Physical security obviously plays a large role in cybersecurity. Concepts like access badges, security cameras, and RSA tokens seem to be the norm. Other physical security measures can include armed guards, locking data in secured storage, bollard’s, and smoke detectors. Using biometrics can also be used for physical security using an eye or even a finger to gain access.

Keeping users well trained has a huge impact on security posture. Having users know and implement safer policies leads to better security. An example of this is often seen by security teams purposely sending out phishing emails. They do this so that unsuspecting employees click on them, and learn of their mistakes. Proactively probing the user base for easily exploited members, while simultaneously training them not to engage with emails that seem to be maliciously crafted. This is a great example of how IT teams actively engage and train employees without scheduling a meeting.

Security is all about mitigating threats. Properly analyzing these treats is an integral part in cybersecurity. At a very high level, one must create a ratio of how much it would cost for the threat to be breached vs how much it would cost to mitigate that threat. Having threats that are not protected leaves residual risk that must be accounted for or passed off to be mitigated through another party.

Authentication keeps data private and restricted to only the users intended to see it. As a web developer this is common using tokens such JWT or homegrown developed tokens. Concepts of cookies play a role in Authentication and in my CEHv9 training we did demonstrations of how stealing cookies could lead to unjust authentication.

1. Knowledge of the human factors in cybersecurity, including human computer interaction, design, training, sabotage, human error prevention and identification, personal use policies, and monitoring.

Humans themselves play an integral role in cybersecurity which has led to the saying “never trust user input”. Making applications interfaces easier and safer for users is a benefit of human factors. Making sure environments are sabotage proof to disgruntled works is another benefit. Having a personal use policy that is implemented and monitored is crucial to make sure there are no gaps in security. Having users that are properly trained mixed with an environment that is both user friendly and secure are the goals of human factors.

c. Ability to identify and analyze problems, distinguish between relevant and irrelevant information to make logical decisions and provide solutions to individual and organizational problems.

I have a clear comprehension and understanding of how to distinguish between pertinent information and data that is irrelevant. This has been shown through my previous role as a VOIP network administrator, communicating issues with client’s point of contacts to help provide solutions to their infrastructure. This has also been demonstrated through my current role as a software engineer by providing dialog in Jira story boards, designing implementations of codes, and creating test steps to help develop more secure and efficient code.

d. Ability to consider and respond appropriately to the needs, feelings, and capabilities of different people in different situations; is tactful, compassionate and sensitive, and treats others with respect.

Respect is crucial in the workplace and having compassion for others while maintaining strict policies can be difficult. This has proven in my previous roles when communicating technical concepts with non-technical colleagues or clients. A lot of these times I had to technically prove out the opposing statements were incorrect, doing that while being tactful yet tasteful. I have been known to engage and create respectful dialog with all people and personally feel as if embracing other cultures, especially in the IT field, leads to a more progressive work environment.

e. Ability to make clear and convincing oral presentations to individuals or groups; listens effectively and clarifies information as needed; facilitates an open exchange of ideas and fosters an atmosphere of open communication.

Public speaking is part of an everyday workplace and is something I excel at. In my current role I have ran meetings on code sprint reviews. Creating open dialog between colleagues while facilitating responses. An open exchange of ideas is what agile development is all about and openly communicating is common through the use of Jira and Kanban boards. Open communication is also performed through reviewing code and leaving comments. In my previous roles as a network administrator, listening skills were paramount. This was because a lot of the times clients were over the phone and you were not able to communicate face to face.

f. Ability to express facts and ideas in writing in clear, convincing and organized manners appropriate to the audience and occasion.

One of my strongest assets is communication, and I feel as if the ability to communicate clearly and effectively is my strong suite. As demonstrated in earlier text, this has been demonstrated throughout my network administration and software engineering career. At a high level working in ticketing systems and creating content that is clear, convincing, and organized while remaining pertinent at hand is the goal of these ticketing systems. These skills have also been expressed through the writing of informative yet persuasive emails to clients and colleagues about code or network administration. An even clearer example of this I have performed is creating documentation and testing steps for applications and IT infrastructure throughout my vocations and not just in a learning environment. Staying on topic while making the information comprehensible is important when writing.