Since my Freshman year in Network Security, I have been very involved in the Information Security Community. While interacting with peers and security professionals alike, I had the opportunity to interact with driven and insightful people all around the world. At any given moment, I could reach out to any of them to either help or be helped.

Shortly after joining the school, I joined a Discord community of students and professionals that come together to learn and teach called Laptop Hacking Coffee (LHC for short). This has brought me closer to the community as it gave me a chance to bond with people all around the world with the same passion for security as my own. It has afforded me the opportunity to learn from people that have worked out in the field for months or years as well as students at the same experience level as myself. The server covers everything from the basics of networking to complex concepts within offensive security. The small community within the server just goes to show how self-driven Cyber Security in its design.

Two years ago, an on-ground club was founded by the name of The Hacking Informational Cyber Crew, otherwise known by its acronym THICC. I became involved in it over time and it strengthened my sense of community because I could immerse myself into an even smaller community of like-minded people, most of whom had the same drive and passion for security. This gave me an opportunity to teach back knowledge that I had been gathering and share with people less experienced as me. Throughout Spring of 2019, THICC hosted an event for building and monitoring honeypots. These are falsified end-users at the edge of a network meant to fool an attacker. The box is created to simulate an end-user in a company and can be used to send an attacker down a wild goose chase while logging and tracking their every move. Because it is isolated on the network, any out of the ordinary traffic to or from the box can be flagged as malicious.

At any given moment, there will always be something that someone wants to have protected. It can be anything from the jewellery they wear to the secure folder on their phone. These opportunities have afforded me more awareness of threat modelling. Threat modelling is the process of identifying and auditing potential risks to themselves, either as an individual or as a company, then creating countermeasures accordingly. A successful threat model will include analysis of any possible effects of these threats and a neutralization strategy. In smaller terms, it is a plan to protect yourself and understand what you are willing to risk losing and what you are not. It can be anything large from whether or not you choose to carry your Social Security card on you or something much smaller like the length of the passcode on your phone. It highly depends on the person what their threat model will look like, thus making it a unique concept. Despite this, it is a concept that is often lost on less security-minded people.