Cybersecurity is a field that has drawn significant attention from institutions, public sector agencies, and private corporations as the demands for well-educated students with exposure to cybersecurity continues to rise. Many collegiate institutions have either established or adopted a fitting cybersecurity education program based on various pedagogical approaches to educating their students in the hope of raising their awareness of security-related topics. Above all, institutions are trying to raise awareness of cybersecurity issues. They hope that through their established programs, students would appreciate cybersecurity and understand the fundamental principle of “security is a continuous process, and not a product.”

In this dissertation, we discuss what needs to be done to increase cybersecurity awareness amongst the younger generations (K-12 students), current cybersecurity educational pedagogical approaches, open-source utilities that are frequently used in cybersecurity education, and additional resources and platforms that instructors may leverage to create their unique educational programs for their students with specific topic interests. We also propose a multi-component adaptive pedagogical framework for the instruction of risk management, incident response, and disaster recovery.

This framework can leverage multiple pedagogical approaches simultaneously to help instructors maximize their instruction efficiency while keeping the students engaged. Specifically, the framework offers traditional power-point slide deck embedded with mini-interactive exercises that reinforces learning as well as take-home exercises through platforms such as EDUrange and the Nice Challenge project that enable students to engage on hands-on laboratory exercises and submit a report for a grade. In addition, there are pre-built surveys and rubrics that instructors may use to assess student learning progress and provide timely assistant should that be necessary to ensure students are up to speed with the newly introduced topics.

The preliminary results of the framework implementation in classroom settings will also be discussed and presented in this work. It is my hope that my contribution to the cybersecurity education field would motivate and spark the interest of other instructors to incorporate cybersecurity concepts early and continuously educate the students the importance of cybersecurity as digital assets, social media and online presence becomes an inseparable part of our lives. Besides that, I hope the content presented within this framework for risk management, incident response, and disaster recovery will become a valuable educational resource that help instructors to educate non-technical individuals interactively and effectively regarding the importance of practicing risk management, and be aware of how to effectively respond to incidents and recover as much lost asset as possible should that be applicable, for it is not a matter of whether they will become the victim of a cyber attack, but a matter of when.