Clarification of the Role of Ethics in the MS Cybersecurity Program

Ethics is a key component of a cybersecurity curriculum. The Cybersecurity Credentials Collaborative (C3) is focused on increasing awareness of vendor-neutral certifications. A key component of these certifications, and a focus of C3, is professional ethics. The University of Arizona’s cybersecurity program was designed to take into account the knowledge requirements of various cybersecurity certifications. Each one has an expectation regarding ethics – both in terms of training and in terms of professional practice. Thus, ethics plays an important part throughout the curriculum.

There are four common core courses in the program. In these courses, two of them have ethics as a key aspect of the course: MIS515 (Information Security in Public & Private Sectors) and SIE571 (Systems Cyber Security Engineering). In MIS515, an entire module is dedicated to discussing cybercrime, ethics, and cyber law. This module represents the equivalent of 6 hours of instruction. In SIE571, topics associated with cyber law and hacking are included. The equivalent of two sessions will be delivered in cyber law, and four to five sessions on ethics – including ethical hacking and unethical hacking, white hat, black hat, and gray hat hackers. In total, this will represent the equivalent of 8-10 hours of instruction. Students will receive the equivalent of 1 credit hour worth of instruction in cyber law and ethics in the core.

In addition to these core required courses, there are other courses in the curriculum in which students will be exposed to issues regarding ethics. Specifically, MIS516 (Information Security Risk Management), which is required in the MIS track, addresses ethics of protecting information and systems. MIS566 (Penetration Testing: Ethical Hacking and Social Engineering), which is required in the MIS track addresses the importance of ethics while learning how to hack systems and social engineer employees; MIS 511 (Social and Ethical Issues of the Internet), which is elective in the MIS track, devotes half the course to ethical issues associated with systems; MIS689 (cyber warfare capstone), which is required in the MIS track, will leverage the capstone position as way of ensuring students have truly learned and understood ethics and its role in cybersecurity. ECE513 (Web Development and Internet of Things) and ECE571 (Fundamentals of Information and Network Security), which are electives in the Engineering track, address designing a system, component, or process to meet desired needs within realistic ethical constraints. Given the C3’s ethics orientation and focus on weaving ethics throughout its certifications, we intend to weave ethics topics throughout the curriculum.

Given its importance in cybersecurity, ethics will be added as a learning outcome and as part of the assessment as follows. The new learning outcome will be “Articulate ethical issues associated with cybersecurity and describe the expectations of ethical behavior by cybersecurity professionals.” We will assess that outcome on exams in relevant courses and behavior assessment in hands-on courses.