

## A Case for Comprehensive, Explicit Ethics Training in Cybersecurity

Denise M. Kinsey, PhD, CISSP, C|CISO

### Abstract:

The ramifications of cybersecurity decisions can range from nominal to life and death. When preparing cybersecurity professionals to make these decisions, educators should ensure that students are prepared with the knowledge and understanding of how to assess the situation and react in an appropriate manner. To achieve that level of competence cybersecurity ethics should be taught in a manner that empowers and prepares students to address those issues. By creating authentic experiences and exercises the student can be immersed in the content and have those memories to reference when a new situation occurs. This paper details the need for interactive cybersecurity education and details the results of an experiment to determine the likelihood of students to behave ethically if there was little chance of getting caught.

Cybersecurity is essentially the “keys to the kingdom” especially when a cybersecurity analyst was hired into that position directly without the opportunity to grow within an organization allowing for vetting of their skills and ethics for alignment with corporate culture. When a student graduates from a cybersecurity program in this country there is often the expectation that the student will know how to behave ethically so as to not embarrass the organization or themselves. After reviewing many cybersecurity programs and aiding in building curriculum at both two and four year schools, there is a lacking of explicit ethics training in many programs. According to Edwards and Gallagher (2018), there are more widespread ethical scandals in the news which brings to mind the question of if ethics are taught and if so, how those standards are taught as the problem is not going away.

When building a degree plan it can be daunting to fit in every important element a student needs to be successful. Incorporating all of the subjects necessary to ensure students understand and can apply the cybersecurity concepts to problems and gain employment in the field is often a difficult task. State and Federal regulations, accreditation boards, advisory boards and school boards and academic standards committees all have opinions or guidelines on what must be included and how the content should be approached while limiting the number of credit hours in which educators can present the content. A degree is not simply focused on the discipline but includes many courses to aid in a well-rounded approach to life separate from the focus of study. It can be a challenge to condense the cybersecurity topics in to logical, cohesive courses and still cover all of the material.

The limited number of courses and the large list of topics within each course can make it appealing to assign some content as reading assignments which are not assessed. The ethics component at many schools has fallen into this category. Required readings may offer the

student exposure to what is expected in terms of ethical behavior but what guarantee is there that he student read the material? Is there verification that they understood it or may be able to recall it if there is a need to apply ethical conduct to a situation?

When ethics is relegated to a 'grocery list' item and not made the focus of curriculum it can easily be overlooked or viewed as tangential to the material as opposed to absolutely essential. Many schools have adopted curriculum that includes subjects like ethics in several courses to identify how the ethical considerations may be applied to each subject. Other schools have it as part of a single course where it is listed in the course description and efforts are made to present information to persuade the student to follow the standards and behave in an ethical manner.

One of the most difficult aspects of applying ethics to a situation is determining whose ethics should be followed. For example, two people raised in the same city, attended the same primary and secondary schools, and come from families with similar social backgrounds may not have similar ethics. Now consider a more diverse population like a college or university. The University of Houston, for example, serves students from more than 130 countries (University of Houston). When considering the second most diverse student population in the country the thought of teaching ethics may feel overwhelming. It can be in much less diverse populations. Elliott, Stokes, and Cao (2018), offer "Western ethics may be difficult to translate into the philosophical concepts common to students from different cultural backgrounds" (p. 359). Ametrano (2014) identified challenges professionals faced "when confronted with what they perceive as conflicts between professional codes of ethics and their own values" (p. 154). This requires we aid students in developing "the 'philosophical sophistication' to reconcile personal and professional values" (Ametrano, 2014, p. 154).

Remembering the ethical foundation, while necessary, does nothing to aid in ensuring implementation by the student. Because of the ramifications of each decision in cybersecurity it is absolutely essential that ethics is taught in all cybersecurity programs. Only explicitly including the relevant connections between student and the ethical principle educators meet the student through both the cognitive and affective lens Bloom introduced.

According to Kirkman, Fu & Lee (2017),

the particular challenge for engineering degree programs is to support the formation of engineers who are not only competent technicians but also responsible professionals, aware of both the ethical dimensions of engineering practice and the broader implications of technological innovation (p. 1).

Why is ethics training important? According to Merriam-Webster (2019), ethics are "rules of behavior based on ideas about what is morally good and bad" (p.1). If the behavior is based on what is deemed good or bad, the determination of how to qualify something as good or bad is essential to learning how one should respond. As much of the application of cybersecurity occurs in the business world a business focused definition of ethics includes "[t]he basic concepts and fundamental principles of decent human conduct. It includes study of universal values..." (BusinessDictionary, 2019, p.1). Once the decision is made to include ethics the focus may shift

to what should be included in the content. While there are many resources that can aid in providing lists of topics, one thing is certain, the content should be relevant, dynamic, and easily understood by the student.

Knowles (2016) notes if for no other purpose, the inclusion of cybersecurity ethics aids in differentiating criminals from cybersecurity professionals as both are often educated or trained in using the same tools or techniques. If the material used to develop skills of those in both categories there should be a means for identification of how it should be used and what constitutes permissible usage and what factors move the activity into inappropriate or illegal usage.

Ethics is often presented as a code of conduct offered by an organization like the ISSA (2019) or SANS (2004). Failure to comply with expected ethics may result in sanctions, revocation of membership, revocation of certifications, public shaming, and other punishments depending on the organization and the level of the infraction. Both of these organizations include language identifying compliance with laws as part of the ethical behavior expectations. Laws may change on a daily basis. If the laws change, what was once permissible may not be any longer.

An expectation of decent human conduct is just as difficult to identify or keep stagnant for the purposes of teaching a consistent message within a scholastic term. The two major political parties in this country are polarized on what each deems is 'decent' behavior. How can a consistent message be formed that will satisfy both parties and all other factions? According to Harman states "there is no single true morality. There are many different moral frameworks, none of which is more correct than the others" (as cited in Budd, 2018).

Edwards and Gallagher (2018) "contend that traditional (i.e. normative) approaches to teaching ethics have largely failed to translate into greater ethical behavior in business settings, and it is important to consider why this is the case" (p. 2). Maxwell and Schwimmer (2016), note the need for faculty to serve as moral models from the early days of teacher education. The authors go on to make a distinction that one should not base their ethical decisions solely on their reactions to the situation as "personal moral intuitions are not necessarily a reliable guide to what society and the profession expect of them in their professional role" (p. 360).

The goal of ethics courses should be assimilation of the concepts including understanding, applying the concepts and controls, analyzing the situation for modification or enhancements, evaluating the effectiveness and potentially creating new solutions. For that to occur the student needs to identify with the situation or be able to find a commonality with their lives or past. How aligned ethically a student may be and the consistency of their decision making process to select ethical options is likely to vary by the student's academic major (Aguirre, Hyman, Goudge, Genchev, Carrell & Hamilton, 2017).

To make the content relevant to students it must be presented in such a way that the students understand it and can find linkages or connections to their lives and experiences. This is similar to many computer programming teachers immersing the students in the language and process by

having them develop programs to solve a problem with relevance to that student. Instead of the teacher assigning a pre-determined problem or assignment from the book, the student must identify a problem, identify potential solutions, design and build one of the solutions to that problem and test if the solution is successful. The act of elevating the content from an 'I told you to do it' assignment to an immersive problem solving, multi-faceted challenge moves the students through several layers of Bloom's Taxonomy to the higher levels. Moving from a knowledge assignment with the required outcome of remembering the material into application of the material, analyzing the problem, evaluating potential solutions, and creating a solution moves students through the layers of Bloom's Cognitive Domain (Vanderbilt, 2019).

Bloom and Krathwohl (Wilson, 2019) proposed the affective domain, another of the three complimentary domains. The affective domain is concerned with emotion in a response to a situation or the level/degree of rejection or acceptance of an action, attitude, or option. Edwards and Gallagher (2018) contend that students are not provided the opportunity to sufficiently practice ethics in most education programs. While they focused on business education the premise is valid for all education when the manner in which the content is presented is considered. Static presentation of material fails to evolve in Bloom's taxonomy beyond the most basic level – knowledge. There is no opportunity for students to apply the material to an authentic situation. Providing students the opportunity to practice ethical behavior in an exercise allows the student to identify the material as fitting into their value system or to reject it.

What constitutes an authentic ethics experiment or experience? Recent presentations at security groups including South Texas ISSA and ISACA Greater Houston chapter, some organizations have taken phishing exercises and cybersecurity awareness training to the next level by hosting in-house testing/experiments where employees are sent phishing emails and if they click on the link they are required to remediate the company policies and anti-phishing training. Some, if an employee repeats the offense, will actually fire the employee.

By incorporating immersive ethic experiments or exercise all three domains are addressed. The linkage between the content and the student's values and responses may be more clearly delineated by stepping through the process. Having 'lived' the process and identifying what the appropriate response should have been the student may assimilate the correct response for recall and repetition the next time an ethical situation arises. To truly understand how one will react to an ethical dilemma or in a given situation it helps to practice situations where problem solving and challenges are posed. According to Weidman and Coombs (2016), a simulation "allows STEM students to plan, adjust their plans to solve problems, and learn the importance of effective communication" (p. 14).

Weidman and Coombs (2016) have identified that "research shows students need to participate in discussions - either as a whole group or as a class – to benefit fully from simulations" (p. 16). This offers insight and perspective. When other students share why they evaluated the situation in a specific way resulting in a limited selection of options and how the options were assessed and one selected all participants are offered a navigated tour of the process through the eyes of a peer and the material may resonate in a way that simply stating one passed or failed the

simulation would not. Students are offered an opportunity to reconsider their selection in light of other options and their peers' selections to further validate the correct or more correct options.

Edwards and Gallagher (2018) culled the literature and found there was little research concerning the motivation level of students who studied ethics. If the course or content is part of a degree program the student may have no choice in whether to study the material or not. Offering ways for the student to experience the material affords the opportunity to make personal assessments of their own choices and behaviors in regards to a given situation.

To provide as authentic an experience as possible several experiments were conducted. These experiments were conducted with full college and IRB approval and were later discontinued upon a single student's complaint. A computer lab (the cybersecurity lab) with clear signage that the lab was under surveillance and that all activities 'may' be monitored was used. The basis of the scenario was basic honesty. Would a student steal a wallet or its contents if no one was looking and there was little threat of being caught?

To set-up for the experiment 100 used wallets and purses were purchased from various resale stores. The college ID office aided in making 5 fictitious student IDs to go into the wallets and aid in identification. None of the IDs were real or based upon a real person. The wallet was either left on the ground near a desk or was in a purse left under a chair or slung over the back of a chair. Within the wallet was a sum from \$2 to \$20 in a combination of bills. Every experiment included miscellaneous other items which could include a bus card (empty- no funds), a college 'cash' card (empty- no funds), movie ticket stubs, note with a date and time, note with a classroom and college class specified, a couple quarters. If a purse was used it include a used lipstick, a hair comb, facial tissue, pens or pencils, a small notebook with some classrooms and course titles scribbled in it, all of nominal value but all used items (except the facial tissue) to denote it was someone's property and not new purchases for an experiment. Over the course of a term, on a variety of days and times, the wallets or purses were left in the unoccupied room prior to one of the cybersecurity courses beginning.

The simplified results of the experiment included two students attempting to return the wallet/purse, with the items intact, to the security office immediately or right after class. Five students placed the wallet/purse in the front of the room at the instructor's desk. Three students ignored the wallet/purse and the teacher pretended to find it as the class in the room afterwards was not a cybersecurity course and therefore not intended for the experiment. All 40 of the remaining students either stole the entire wallet/purse or removed the wallet from the purse leaving the purse, or removed the cash and/or cards from it and discarding the wallet or purse where it was found or in the trash. Two students from the class were never engaged in the scenario but all others in the two classes were. Needless to say, the results were very disappointing. At the end of the semester the results (anonymized) were shared with the class. One student was so outraged that he made a scene in the class and then later complained to the chairperson and provost. The experiment was ended at that point by the administration. The only way the class knew his unethical choice in the exercise is because of his behavior. Otherwise no one would have known which students made which choice.

The experiment has been repeated since that time but on a much smaller scale. There have also been additional experiments where opportunity thefts could occur or a 'test key' was intentionally left on a monitor while the teacher walked away. Roughly 70% of the students copied the answers or took photos of the screen, or printed the page. A few even sent it to themselves as email attachments. One of those students failed to delete the sent item from the sent box.

The assumption that students will perform ethically on the job or when making serious decisions is flawed when students make unethical decisions as a matter of habit. These results are not isolated. Kirkman, Fu & Lee (2017) found that students improved in ethical challenges, problem solving, and decision making after a problem was posed they were instructed to solve. Upon selecting and defending a solution, the authors identified key areas of strength or unethical behavior in the selection. Students were given the opportunity to talk through their reasoning and learn from their choices. This allowed for improved scores on the next challenge (unrelated to the earlier challenge) and increased satisfaction and self-efficacy. Ametrano (2014) noted that after immersion experiments, "the most notable changes were evident during the semester were in student's strategies for making ethical decisions" (p. 156).

Ametrano (2014) highlights that "professionals are not expected to be without bias, but they are expected to engage in self-examination so that their biases can be evaluated, wrestled with, and ultimately reconciled with the standards of the profession" (p. 15). The best way to do that is to place students in ethical dilemmas where they must figure out the correct choice or develop a solution. Ametrano (2014) offers a variety of options for these experiences "this may be accomplished by having students apply information in case studies, role-playing, discussion and interaction with peers, and self-reflection" (p.155). The benefit of pre-planned immersive experiences is "students learn there are few clear-cut answers but they can be systematic in their decision making and learn to recognize better choices" (Ametrano, 2014, p. 155).

Many faculty have complained lately about an increase in cheating from both undergraduate and graduate students in various computer science and engineering courses including cybersecurity. The ease by which many students cheat on their schoolwork is another reason for teaching ethics as an intentional, explicit subject within the curriculum. All educators should endeavor to educate students on cybersecurity ethics because after all, the students trained in our programs will secure our retirement homes.

#### References:

- Aguirre, G., Hyman, M.R., Goudge, D., Genchev, S., Carrell, A., and Hamilton, C. (2017). Teaching ethics to marketing and logistics majors: A transformative learning experiment. *Journal of education for business*
- Ametrano, I.M. (2014, April). Teaching ethical decision making: Helping students reconcile personal and professional values. *Journal of counseling & Development* 92(4). American Counseling Association. p. 154 -161.

Budd, J.M. (2018). Teaching Ethics: A Framework for Thought and Action. *Journal of Education for Library and Information Science*, 59(3), doi: 10.3138/jelis.59.3.2018-0022.06

BusinessDictionary (2019). Ethics Definition. Retrieved from <http://www.businessdictionary.com/definition/ethics.html>

Center for Teaching (2019). Bloom's Taxonomy. Vanderbilt. Retrieved from <https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/>

Edwards, M.S. and Gallagher, E.C. (2018). Oh, Behave! Insights and strategies for teaching business ethics to gen Y students. *E-Journal of Business Education & Scholarship of Teaching* 12(1). Pp: 1-18.

Elliott, A. C., Stokes, S. L., & Cao, J. (2018, Nov). Teaching ethics in a statistics curriculum with cross-cultural emphasis, 72(4) p. 359-367. Doi: 10.1080/00031305.2017.1307140

ISSA (2019). ISSA Code of Ethics. Retrieved from <https://www.issa.org/page/CodeofEthics>

Kirkman, R. and Fu, K., and Lee, B. (2017, Fall). Teaching ethics as design. *Advances in engineering education*, pp: 1-16.

Knowles, A (2016, Oct 12). Tough challenges in cybersecurity ethics. *Security Intelligence* (Securityintelligence.com)

Maxwell, B. and Schwimmer, M. (2016). Professional ethics education for future teachers: A narrative review of the scholarly writings. *Journal of Moral Education* 45(3) pp 354-371. Routledge.

Merriam-Webster (2019). Definition of ethic. Retrieved from <https://www.merriam-webster.com/dictionary/ethic>

SANS (2004). IT Code of Ethics. SANS. Retrieved from <https://www.sans.org/security-resources/ethics>

University of Houston (2017). Retrieved from <http://www.uhsystem.edu/uh-system/uh/>

Weildman, J. and Coombs, D. (2016, April). Dodging marshmallows: Simulations to teach ethics. *Technology and engineering teacher*. Pps 14-18.

Wilson, O. (2019). Three Domains of Learning – Cognitive, Affective, Psychomotor. The Second Principle. Retrieved from <https://thesecondprinciple.com/instructional-design/threedomainsoflearning/>