# Embedding professional practice into the cybersecurity curriculum using ethics.

FAILY, S. and JONES, M.

2015

# Embedding Professional Practice into the Cybersecurity Curriculum using Ethics

Shamal Faily
Department of Computing & Informatics
Bournemouth University
Poole BH12 5BB, UK
sfaily@bournemouth.ac.uk

Michael Jones
Department of Computing & Informatics
Bournemouth University
Poole BH12 5BB, UK
mwjones@bournemouth.ac.uk

***Abstract*— Cybersecurity graduates are ready to tackle the technical problems they might face, but employability needs to be incorporated into the curriculum should they wish to tackle ill-defined professional challenges as well. We describe how employability was incorporated into the cybersecurity curriculum by teaching ethics and ethical problem solving as part of an undergraduate module on *Ethical Hacking & Countermeasures*. These changes were critically analysed using the USEM account for employability, together with principles for work-based learning assessment.**

## I. Introduction

Cybersecurity is a growth area of employability for new graduates, but are we preparing tomorrow's cybersecurity graduates for the contemporary challenges faced by cybersecurity practitioners? While new graduates are equipped with the technical knowledge required to tackle these problems, they may not be sufficiently appreciative of the professional challenges they might be expected to face. Preparing students to face these challenges is a burden that universities are increasingly expected to shoulder, and not only by employers. Students want professional experience that give them an edge over their peers in the job market, and parents consider employability when considering the return on their child's investment in university education.

Employability is written into university strategic plans, but incorporating it into curricula is easier said than done. Identifying real-world projects that are complex enough to be useful, but simple enough to be understandable is challenging. Moreover, given that cybersecurity remains an emergent area in terms of research, practice, and education, employers may also find it difficult to frame project opportunities suitable for students, particularly because some employers have security requirements, but lack security expertise [1]. Employability is also one of the many tensions that academics need to contend with, with some academics considering it an intrusion to academic life [2]. Such tensions become even more strained when considering that, as a result of the marketisation of Higher Education (HE), some HE professionals are starting to consider employability as a goal of HE, rather than a measure of its quality [3].

If students are to successfully identify the root causes of ill-defined security problems found in practice, they will need to demonstrate creativity given the legal context that constrains their environment. Ethical principles and problem solving demonstrates this creativity by fostering critical thinking. It achieves this by helping to classify arguments, defend a position or better understand the position others take and, in doing so, determining appropriate courses of action for resolving such ill-defined problems [4]. Thinking about what it means to be ethical means thinking about the consequences of commercial decisions that students face as penetration testing practitioners. Such decisions range from agreeing the parameters of a security test, to deciding what activities should or should not be part of the test [5]. Understanding legal issues is necessary, but not sufficient for dealing with such decisions. Some decisions might be legal, but potentially unethical. While the necessity to attend to ethical considerations is broadly accepted, guidance on how to do so is not.

## II. Our Approach

We incorporated ethics into the cybersecurity curriculum by making modest additions to our second year undergradute *Ethical Hacking & Countermeasures* unit. Material on ethics was incorporated into a pre-existing lecture on Legal and Ethical Issues. The idea of a 'fallacy' was introduced to students, together with common fallacies held by some hackers, such as all information should be free, break-ins illustrate hitherto ignored problems, and hackers are keeping 'big brother' at bay [6]. The lecture then presented existing material on the most relevant pieces of legislation related to hacking, before discussing issues relying on codes of practice alone for ethical guidance. The students were then presented with a three step approach for resolving cyber-ethical dilemmas [4], and introduced to the strengths and weaknesses of several common ethical theories, such as consequentialism, deontologism, and relativism.

This material was formatively evaluated in a two hour seminar accompanying this lecture. The seminar entailed the class dividing into small groups to answer two questions. The first question required students to answer the question 'is ethical hacking an oxymoron'. Students were required to apply the three-step process presented in the lecture. The second question, which is drawn from [4], asked students to compare and contrast the thought processes associated with breaking

into a car to drive a friend to hospital who might otherwise die, and breaking into a computer to obtain medical information that would save the friend's life. To answer this question, the students were required to analyse the three-step process presented, together with the fallacies discussed by [4]. After 90 minutes, the groups came together to present their answers, and receive criticism from other groups about any ambiguity or fallacies evident in their results. By learning about fallacies associated with unethical hacking decisions, and making sense of ethical dilemmas in the safe environment of group seminars, these changes also led to the addition of 'unethical hacking practices' to the unit's "null curriculum" [7]. Such practices might have been otherwise afforded by the technology used by students on this unit.

The material was summatively evaluated using a coursework assignment. This assignment was modified in two ways to not only support the teaching of ethics, but the embedding of professional practice in general. First, the coursework was designed to explore what it means to evaluate security for two target systems – one technical, one socio-technical – in the contemporary, but ill-defined commercial context of start-ups. Start-ups need to be highly innovative if they are to capture market share, but they also need to demonstrate assurance in their software and their business operations to attract prospective funders. Second, 40% of the coursework was based on activities that required them to resolve simple ethical dilemmas. Although the coursework brief was situated around a hypothetical start-up, students were required to collect and analyse open-source intelligence about local incubation space providers where the start-up might be based. This analysis would be fed into the design of hypothetical scenarios for obtaining physical access to hardware at the incubation provider's site.

## III. Results

### A. Employability claims analysis

We critically analysed our approach by considering the employability claims using the USEM (Understanding, Skilful practices, Efficacy beliefs, and Metacognition) account for employability [2].

The coursework assignment already incorporated elements of metacognition because students were required to reflect on the risks identified in order for them to describe their implications to the [albeit hypothetical] client organisation. However, introducing ethics into the curriculum helped students understand the differences between 'ethical' and 'non-ethical' hacking. While students initially thought that 'ethical hacking' might be oxymoronic, asking if they were behaving ethically in attending such a course successfully cast doubt over pre-conceived ideas they might have had. Because critical thinking is necessary to resolve ethical dilemmas, students also discovered that procedural 'problems solving' skills hitherto used only to tackle technical issues could also be used to address social issues. Moreover, by solving such problems, students demonstrated self efficacy by producing legally and morally sound results in what might be considered a legally risky area.

### B. Summative assessment evaluation

As well as evaluating the curriculum changes in general, we also considered how well the summative assessment addressed validity, reliability, and authenticity principles for work-based learning assessment proposed by [8].

The assignment had content validity because the ethical challenges faced in this assignment are not dissimilar to those faced by penetration testing practitioners based on recent research on ethical dilemmas faced by penetration testers [9], however it lacked a certain amount of predictive validity; this is because students would not normally be expected to resolve the dilemmas faced in the assignment on their own, and would benefit from guidance from their leaders and, quite often, mentorship from more senior staff members in their firm. Existing quality assurance practices demonstrated asssessment reliability, and – although there was some evidence students shared ideas about approaching the assessment – the assignment satisfied authenticity principles. This is because the assignment was designed in such a way that successfully committing an academic offence would be difficult due to the requirement to explain the thought processes behind the evaluation of each target. This would be evidenced in the presentation of risks in the technical target, and an explanation of how the scenarios presented in socio-technical target was grounded in the information gathering and analysis activities individually conducted.

## References


[1] D. Gollmann, *Computer security*, 2nd ed. John Wiley & Sons, 2006.

[2] P. Knight and M. Yorke, *Learning, Curriculum and Employability in Higher Education*. Routledge, 2003.

[3] F. Valenzuela, "On employability in higher education and its relation to quality assurance: Between dis-identification and de-throning," *ephemera: theory & politics in organization*, vol. 13, no. 4, pp. 861–873, 2013.

[4] H. T. Tavani, *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology*. John Wiley & Sons, Inc., 2006.

[5] M. Bishop, "About penetration testing," *Security Privacy, IEEE*, vol. 5, no. 6, pp. 84–87, Nov 2007.

[6] E. H. Spafford, "Are computer hacker break-ins ethical?" *Journal of Systems and Software*, vol. 17, no. 1, pp. 41–47, Jan. 1992.

[7] E. W. Eisner, *The Educational Imagination: On the Design and Evaluation of School Programs*, 3rd ed. Pearson, 2001.

[8] D. Gray, *A Briefing on Work-based Learning*. LTSN Generic Centre Assessment Series, 2001.

[9] S. Faily, J. McAlaney, and C. Iacob, "Ethical Dilemmas and Dimensions in Penetration Testing," in *Proceedings of the 9th International Symposium on Human Aspects of Information Security & Assurance*. University of Plymouth, 2015, to Appear.