Teaching Psychological Principles to Cybersecurity Students

Assoc Professor Jacqui Taylor, Dr John McAlaney, Sarah Hodge, Helen Thackray, Dr Christopher Richardson
Faculty of Science & Technology,
Bournemouth University
Poole, UK
jtaylor@bournemouth.ac.uk

Susie James, John Dale
LiMETOOLS Ltd,
Bournemouth, UK

***Abstract*— This paper will discuss our observations gained from teaching psychological principles and methods to undergraduate and postgraduate cybersecurity students. We will draw on and extend our previous work encouraging the teaching of psychology in computing and cybersecurity education. We pay special attention to the consideration of characteristics of cybersecurity students in terms of teaching psychology in a way that will be accessible and engaging. We then discuss the development and use of an online training tool which draws on psychology to help educators and companies to raise awareness of cybersecurity risks in students and employees. Finally, we offer some practical suggestions to incorporate psychology into the cybersecurity curriculum.**

Keywords—psychological; cybersecurity; social engineering; higher education; social psychology; cognition

I. INTRODUCTION

The format for the paper is as follows. Section two will briefly review literature that highlights what psychology can offer to computing and cybersecurity education; further published research will be presented within the following sections. Section three will then review some of the ways that we have been involved in teaching psychology to cybersecurity students, at undergraduate and postgraduate level. Section four will highlight how an understanding of the characteristics of cybersecurity students has been considered to adapt existing teaching materials used with psychology students. Section five will discuss the development and subsequent user testing of a new interactive multimedia tool to teach behavioural aspects of cybersecurity to students, academics and industry. User trials with students have identified some of the key requisites for successful cybersecurity self-directed learning programmes. The conclusions, covering some practical suggestions, are presented in section six.

II. WHAT CAN PSYCHOLOGY OFFER TO CYBERSECURITY EDUCATION AND TRAINING?

There is a symbiotic relationship between the disciplines of Computing and Psychology: psychologists have helped in many ways to understand the way that computer systems are developed and used, but also an understanding of computers has helped psychologists to model and investigate human cognitive and social processes. This paper will focus on the former; over the past 60 years, psychologists have tracked and researched the development and impact of computers and they have also been instrumental in their design and evolution. To design, develop, implement and evaluate secure sociotechnical systems students need to understand elements of cognitive and social psychology.

To understand the potential risks of sociotechnical systems, cybersecurity students need to understand and consider how people perceive, remember, feel, think and solve problems, i.e. the domain of cognitive psychology. It is also important for students to consider individual differences and social behaviour if effective interaction between people and computer systems is to be achieved, i.e. the domain of social psychology and individual differences. An understanding of these psychological topics enables students in cybersecurity to consider the potential capabilities and limitations of computer users and helps them to design computer systems that are more effective (usable) for a variety of user types. In addition to covering the foundation areas of Psychology, it is also important that cybersecurity students are taught evaluation methods and that they are able to consider the social impacts and ethical issues regarding the implementation and use of computer systems in organisations and society.

A review of the literature and media commentary on cybersecurity attacks shows that increasingly they involve social engineering techniques; where psychological principles are used to manipulate people into disclosing sensitive

information or allowing others to access a secure system [1]. For example, phishing emails and phone scams utilize many psychological principles relating to social influence to persuade users to open a link, such as appeals based on fear or invoking a sense of scarcity or urgency [2]. However, despite the psychological nature of such cybersecurity attacks, research into the role of psychology in cybersecurity is still limited [3]. Also, often research into the closely linked area of social engineering is conducted from the discipline of computing rather than psychology. Indeed the call for papers for a recent conference organised in the UK by the Higher Education Academy on learning and teaching in cybersecurity listed relevant disciplines as 'STEM' and 'Computing' and the eventual programme of abstracts contained no mention of psychology. Similarly, curricular guidance for the field of cybersecurity education produced by the ACM [4], contained just two uses of the word psychology and no further detail. However, within the last year the importance of psychology has begun to be recognized in the academic literature [3]. An article published this year [5] suggests the teaching of game theory in cybersecurity courses and links this to the psychological nature of many incidents. They propose that one of the benefits of game theory is that it fundamentally alters the way students view the practice of cybersecurity, they state that it helps "to sensitize them to the human adversary element inherent in cybersecurity in addition to technology-focused best practices" (p1).

The majority of psychological research that has been conducted so far in this area has focussed on prevention and mitigation strategies for the targets of cybersecurity incidents with little focus on the motivation of the perpetrators [6]. Psychology can offer much in helping to understand the motivations of individual hackers or scammers, for example drawing on the research into individual differences, looking at factors such as self-esteem, introversion, openness to experience and social anxiety [7]. Other work has shown that individual's motivations are not always related to financial gain but can be purely for entertainment or social status reasons [6]. In contrast, large scale cybersecurity incidents are often instigated by groups, as opposed to individuals acting alone. As such these incidents can be regarded as the result of group actions and group processes; theories from Psychology are used to help understand the formation, operation and influence of groups on their members, and these can be usefully applied to online groups [3]. Many hacking incidents, especially those perpetrated by teenagers and young adults, have been strongly related to social group pressure and social psychological influences. For example, individuals involved in the 2015 TalkTalk and 2011 Paypal hacks were instructed on how to do this by members of Anonymous, the hacktivist collective.

Psychological theories relating to disinhibition and deindividuation have been used to explain a number of behaviours online and can also be used to understand cybersecurity incidents. The perception of anonymity afforded by online communications allows individuals to take actions that would otherwise result in legal or social sanctions. Disinhibition refers to the sense that actions conducted online do not feel as real as those conducted offline which, it has been argued, can lead individuals to lose self-control [8]. Deindividuation, in which individual lose their sense of self-awareness when they interact within a group, has been applied to online groups where individuals are often less identifiable and separated by space and time [8]. This is an under-researched area, but it would seem that, in line with Social Identity Theory, some individuals become engaged with online groups to an extent which would seem to be particularly intense and where they lose some sense of personal identity to social identity. In summary, theories from psychology can be helpful to understand and help to predict online behavior.

III. Experiences Teaching Psychology to Cybersecurity Students

In this section, we will review our experiences teaching psychological principles to a wide variety of cybersecurity students. We have experience teaching at undergraduate and postgraduate level (full-time and part-time), short courses for CPD and developing cybersecurity training tools for industry. Foundation areas in Psychology which we consider important to introduce to students prior to discussing their application in cybersecurity are: social processes (e.g. group-working and communication); cognitive processes (e.g. perception, attention and memory), and individual differences (e.g. life experiences, gender, personality, cognitive style). Once these areas of psychology are covered, then it is easier to show how we apply psychological principles to cybersecurity.

A. Social Psychology and Cognition

The work of social psychologists can help understand the ways that technology affects social interaction, attitudes and behaviour. As we have taught mainly part-time, 'mature', employed students we ensure that there is a strong focus on how students can make practical use of the research findings in their own work. We cover the major topics within Social Psychology (conversation and communication; group processes; interpersonal perception and attraction; social influence; attitudes, and conflict) and Cognitive Psychology (perception, attention and memory). Then we apply this understanding of social cognition to cybersecurity contexts. Topics we have covered include:

i) how an analysis of online language and communication can be used to identify fraudulent communication and how persuasive language can influence faulty decision-making regarding judgments of trust;

ii) group dynamics in cybersecurity actors are reviewed, for example the group processes that shape the actions of both the cyber attackers and their intended target, including how group dynamics may lead to risky decisions and overestimations of skill and ability;

iii) the psychological basis of social engineering techniques, and how these may be mitigated and prevented;

iv) the role of emotion when users engage with sociotechnical systems, e.g. frustration experienced with the technical components of a secure system have been linked to poor decision making and subsequent risky behaviour;

v) the link between cognitive load and poor online decision making;

vi) new technology and organisational change is highlighted, covering issues such as the management of staff working remotely online and online methods for recruitment and selection and technology enhanced training of cybersecurity personnel (see section 5), and

vii) the psychological elements of computer games are covered, in terms of the way gamification is used to motivate and persuade potential victims of a scam and also we highlight elements of addiction that may lead to poor decision-making.

Assessment and practical activities are varied and three examples are included here. The ways that online groups can influence the way their members interact and behave is addressed by asking students to devise their own scam website which aims to adopt new members to a fictitious online community. Students design experimental materials to study the links between working memory and online search strategies. Finally, students use and evaluate an online training package to highlight cognitive biases in cybersecurity.

B. Individual differences

To illustrate individual differences in susceptibility to scams, we cover the following:

i) a psychological understanding of the cognitive deterioration in older adults and how this knowledge can be used to understand how, when and why older adults are vulnerable to financial scams;

ii) how gender and personality can affect levels of online susceptibility in relation to internet dating scams;

iii) how stress and cognitive style can influence poor decision making; and

iv) research from consumer psychology related to e-commerce, e.g. individual consumer behaviour and trust in e-commerce exchanges and relations between company and consumer.

In seminars, cybersecurity undergraduates engaged well in tasks where they were asked to think from both the defence and attack perspectives. For example they were asked to identify the most at-risk groups and then tailor the advice they would give to that specific group. For example, if they are advising an older adult who is unfamiliar with technology, they must think of how to explain this using simple terminology. If explaining to a child how to stay safe online, they need to use examples that children can identify with. Students were also asked to design a cyberattack that would circumnavigate their advice. The most successful exercises were highly interactive; recapping information from the most recent lecture, discussing in groups and then presenting their viewpoints to the class as a whole. It was interesting to see that despite beginning the module with a somewhat cynical attitude to the importance of psychology, after a few seminars there was an increase in interest and participation. One large consensus from the students was that there needs to be greater emphasis on education about cybersecurity at all ages and levels of experience.

C. Research methods

Cybersecurity students may have limited understanding regarding the way empirical methods (an integral part of all Psychology degrees) can be used to evaluate computer systems. To address this, topics such as Experimental Design and Internet-Mediated Research are covered. Ideally students need to experience or apply methods, therefore it is helpful if the teaching experience includes case studies and practical workshops and assessed scientific reports. We have run workshops which compare qualitative methods (e.g. observation, focus groups) and quantitative methods (e.g. questionnaires and performance scores) to evaluate the individual's perceived vulnerabilities and this has contrasted the different methodological approaches well.

Designing an Internet-based experiment or survey requires careful consideration. Although cybersecurity students clearly have the technical skills to conduct online surveys, they often have less understanding of experimental design and what can be done with the data. There are many benefits of Internet-mediated research (for example, access to a larger population), however, many psychological and methodological issues need to be addressed by cybersecurity students and researchers. Issues we cover include:

i) the difficulty in ensuring that the participant is who they say they are and that they are answering in an honest way;

ii) how to gain a representative sample;

iii) how to construct questionnaire items to avoid bias;

iv) issues of data screening and sample attrition rates need to be considered;

v) the demographic profiles and questionnaire scores of those who did and did not take part in online experiments or surveys need consideration, and finally

vi) ethical issues, e.g. whether informed consent can be gained online and how debriefing will take place (covered more fully next).

D. Ethics

The teaching of ethics to cybersecurity students is not new. For some time, the teaching of ethics has been a requirement on degrees accredited by the British Computer Society (BCS). Since the classic text on computer ethics [9], coverage of ethics has increased as computer systems become more pervasive in daily life. For example, issues of information security such as privacy, ownership, access and liability and reliability have become more important. These advances have led to the most recent edition of computer ethics [10] including much work drawing on Psychology, e.g. covering the psychological and

social implications of Internet use. However, despite the increasing need for ethics teaching sometimes there can be pressure on Computing departments in meeting this requirement. This is mainly due to it being a difficult area for computing staff to teach which, according to [11], is because the area of ethics is not positivistic in nature. As psychologists we have been able to offer a different perspective on ethics to cybersecurity students, based on the work of [11], who discuss the use of educational theory and moral psychology to inform the teaching of ethics in computing-related fields. In their paper, they discuss ideas on moral development and the nature of morality, specifically as it relates to changes that educators may be trying to elicit within computing students when teaching ethics. The ways that a computer scientist and a psychologist teach ethics can be quite different, with the former more likely to use a positivist approach and the latter an approach based on educational theories. For example, a positivist approach would define what is right and what is not right (i.e. define truth) and then address what happens if one does not do what is right or does what is wrong. However, many Psychologists would disagree, saying that you cannot teach right and wrong and that although there are many laws which computer students need to know about, regarding what is wrong/right in society, there are not many things that are ethically questionable that are not illegal (and possibly vice versa!). In summary, philosophers have long recognized that it is almost impossible to 'teach' a student ethics, rather teachers need to advance students' sense of moral development and reasoning [12], something covered on all Psychology degrees. With this in mind, it is also important to consider the age and experience of students when designing teaching materials on ethics (covered further in section 4). In summary, Psychologists have a lot to offer in the teaching of ethics to cybersecurity students. Some academics [13] go as far as discussing ethics purely in psychological terms, regarding the cognitive, affective and social aspects, when they state that the origins of human morality are 'emotions linked to expanding cognitive abilities that make people care about the welfare of others, about cooperation, cheating and norm following'.

Considering the importance of individual's own behaviour around security and their understanding of the implications and consequences of behaviour, the behavioural component of morality could be of great value to teaching psychological principles to cybersecurity students; especially as learning has been shown to be aided by doing [14]. Utilising educational games such as the Cyber Security Challenge UK has been of great value; such games set challenges for students to complete such as finding hidden data within a spread sheet. Additionally, we draw on students' life experiences to aid learning of the psychological materials; discussed further in the next section.

IV. Consideration of the Profile of Cybersecurity Students in Developing Psychology Materials

The variation between students studying different disciplines has been well documented regarding life experiences, gender and approaches to studying [15]. It is proposed that some of the following factors may affect the way that psychology teaching materials are perceived and understood by cybersecurity students and their level of engagement with the materials. Without wishing to generalise, these factors were considered in the way that materials were designed and presented.

A. Gender

The composition of most Psychology and Computing degree courses are significantly skewed, with females making up the majority of psychology degrees (79.4%) and males making up the majority (82.6%) of computing degrees [16]. There have been many attempts to explain the reasons why males and females are attracted to different disciplines and a review of these studies shows very little support for cognitive abilities being the differentiating factor; for example, similar abilities have been found when comparing students studying social with physical sciences [17]. Recent research has looked at personal values, interests or motivation factors to investigate what [18] term, 'what people want to do rather than what they can do'. Wilson [19] used quantitative and qualitative methods to further understanding of how Computing is perceived. In her paper she argues from a constructionist approach that, rather than any real difference in skill, female and male differences are a 'product of historical and cultural construction of technology as masculine' (p. 128). For example, she notes that girls at school have been shown to be superior to boys in some areas of programming, but that they lack encouragement and interest so that by the time they reach 18 years of age they have already opted out. Wilson [19] identifies teaching styles which appeal to female students as those with an emphasis on relational and contextual issues and co-operative learning through teamwork and group projects. While styles preferred by males are those that emphasise the formal and abstract and independent learning. Therefore, when teaching psychology to cybersecurity students (where there are usually more male students) traditional methods used in Psychology classes such as seminar discussions have not always been the most effective method. We have tried to use a broad range of methods, but recognise that some are more effective with the majority male cybersecurity students.

B. Life experiences

Cybersecurity postgraduate and CPD courses tend to attract a significant number of mature entrants who have frequently been employed in other careers, have many life experiences or are currently working in a related industry and studying part-time. It is important for the contextual examples to link to real security incidents and to draw on the experiences of students. While undergraduate cybersecurity courses are more likely to attract direct-entry students, therefore the examples may be more closely linked to incidents publicised in the media.

It is important to consider stage of moral development and life experience of students when presenting materials on the topic of ethics. For example, an environment needs to be created that allows students to safely reflect on and explore their moral beliefs relative to the current issues in cybersecurity. We found that postgraduate students are more interested in the philosophical debates regarding the psychological and legal implications of Internet use, compared to undergraduate students. Issues that students have debated include:
Is deviance online any different from deviance in face-to-face contexts?
Can people become addicted to the Internet in the same way as other addictions and how does this impact security vulnerabilities?
How does a person's face-to-face identity differ from their e-identity?

Gibbs, Basinger & Fuller [20] suggest undergraduates' moral development is not fully developed; they are still developing an understanding of how moral issues may relate more generally to societal functioning. This could explain differences in debates between undergraduates and postgraduates. The postgraduate students were more open to different perspectives than undergraduates and his could be due to being older, and therefore having stronger convictions formed, or life experience within the industry. Thus this could also be informative to the types of materials used to teach psychological principles; the postgraduates may find it easier to consider the bigger picture and societal implications of cybersecurity. While undergraduates may need more support in understanding the wider societal implications.

C. Motivation to Study and Learning Style

The motivation of students to study a particular course will clearly affect their engagement and there may be some initial resentment of cybersecurity students toward the topic of psychology; this needs to be considered and addressed. Many students choose psychology to help develop an understanding of themselves and others and to develop 'people' skills useful later in a range of careers. In contrast, from our observations many cybersecurity students see the course as a stepping stone to gaining almost immediate employment in the security industry or as CPD to gain promotion.

Radford & Holdstock [18] investigated differences between reasons why students chose Computing and Psychology degrees. Students were given a list of 60 items on the 'outcomes or benefits of Higher Education' to rank. These ranged from passing exams, learning to work with others, development as a person, develop problem solving skills etc. The results showed that the most important items differentiating the two fields were that computing students chose the development of problem-solving skills, logical thinking and increasing future earning power. While for psychology students, development as a person was important as was understanding other people, oneself and greater personal independence. They identified two key factors related to choice of discipline: (i) personal development versus social relationships and (ii) thinking about and directly dealing with people versus things. The implications of this for teaching psychology to cyber students are twofold: (i) that cybersecurity students may be less open to thinking about people problems when considering online threats and security, and (ii) that it is important that students are aware of the way people use technology and their interactions with others can be as important as functionality.

A considerable amount of work has been published on the relationship between personality type and learning in Further and Higher Education, although there is relatively little focussing on students from specific disciplines. Layman et al [21] collected personality types of students studying a software engineering course using the Myers-Briggs Type Indicator (MBTI). We considered this when adapting our psychology materials from those designed for psychology students, in terms of: groupwork and individual work; using lectures to emphasise concepts as opposed to factual data, and materials presented objectively as matters of fact with concise, concrete explanations.

It is important to recognise that students studying for cybersecurity courses are likely to have been taught in different ways and may approach studying in different ways, compared to those studying for Psychology degrees. From personal observation, cybersecurity students are generally more familiar with assessments which have definitive answers, while Psychology students are more accustomed to discussing the relative merits of both sides of a debate and to provide a balanced view rather than a definitive answer. This would support the extensive work by [22] investigating learning styles and subject discipline. Depending on their background it has also been our experience that cybersecurity students can find the methodological approaches used in Psychology to be quite different from what they have previously experienced. Students from a cybersecurity background may be more accustomed to an epistemological and ontological stance which posits that understanding of phenomena is reached though objective study and experimental methods, and there is a finite set of solutions to any problem. In contrast the sub-disciplines of Psychology range from those which take a very positivist approach to those which are based largely on ideographic knowledge and social constructionism. Whilst the psychology topics that we have taught cybersecurity students do tend to lean more towards those which take a positivistic approach there is in general more subjectivity and uncertainty embedded with the teaching materials than they may be accustomed too. A comment that we frequently receive from cybersecurity students is that they find it strange that many areas of psychology have no single theory that is widely accepted as being the 'correct' one, and that instead there appears to be often be a multitude of, at times mutually exclusive, theories for any given psychological phenomenon.

V. DEVELOPING A NEW CYBERSECURITY TRAINING TOOL USING PSYCHOLOGICAL AND PEDAGOGICAL BEST PRACTICE

Many of the learning outcomes emerging from teaching psychology and cybersecurity are now being commoditised into commercial tools that can lower risk and increase the intellectual capacity of both large and small businesses. LiMETOOLS is a publisher of learning tools that bring about behavioural change in areas of high commercial risk management, cybersecurity being one. They use aspects of social cognitive theory (SCT) [23], allowing workers to observe a model performing, as in a poor cyber behaviour and the consequences of that behaviour. They use interactive drama to make these scenarios become compellingly realistic and then having immersed the learner, they interrogate them using gaming techniques to explore what they would do next. The staff and managers remember the sequence of events, the video documentary real life case studies and their quiz scores. They then use this information to guide subsequent behaviours. Observing these scenarios can also prompt the learner to engage in behaviour they already have learned, but forgotten, thereby 'nudging' them back to good behaviour.

Before considering the exact content and procedures within the tool, the developers had to understand in more detail the profiles of the target users. Working with small and large groups of students, the developers began to capture measures of general self-directed learning behaviour. These sessions determined the average level of understanding, absorption speed of complex information and simple analytical skills. Initially, this was relatively easy, using traditional techniques. However, the challenge for the developers was to re-measure these behaviours with four distinct variables in action:
(i) behaviour variables that occur in self-directed learning in large, busy, open plan office environments;
(ii) behaviour variables that occur when learning using a mobile device;
(iii) behaviour variables that occur when required to exceed 30 minutes concentrated activity, and
(iv) behaviour variables that occur when working at home.

It became clear that learning in a busy open plan environment required the user to be given information and control of their own progression through the course. They needed to know that the session they were about to experience lasted, say fifteen minutes and required them to put their headphones on to receive audio. The developer's User Profiles indicated that this element of student controlled progression was essential in this environment.

The tablet and mobile interface did make a difference to the manufacturing of the narrative parts of the course. The design of graphical interactive interfaces needed to accommodate smaller screen sizes than a traditional PC, often breaking up user actions into several different screen presentations, rather than just one. Even the craft skills in producing the short documentary videos needed to be adapted to be more 'mobile friendly'.

The developers discovered the level of concentration in self-directed learning dipped quickly after 30 minutes. This was usually because the build-up of emails or the desk phone lights blinking became an increasing distraction to the learner. As time went on, the learners felt the need to manage these intrusions and this required that they Save & Return the programme, thereby losing important focus at a critical time.

Home working analysis presented the developers with a range of options. For some users, their performance was consistently higher when working at home than at work. For others, their performance dropped dramatically. Anecdotal evidence suggested that this was because of family distractions. There were also indications of users cheating in the quiz sections when at home, using Google on another device.

The developers incorporated design changes into the tool specification to accommodate these variables. The biggest challenge in this process was defining the learning journey to ensure a maximum user time of thirty minutes, whilst maintaining balance and appropriate measurement. By making the drama interventions shorter, it was likely the 'stickiness' of the tool would diminish, losing the learner's concentration. On the other hand, shortening the quiz sections would potentially lead the user to believe they had absorbed more than they had actually understood, leading to some complacency and inaccurate measurement. The compromise was made in removing one quiz intervention completely, but toughening up and lengthening the final test and outcome assessment.

On small group testing, using graphical storyboards, the most attractive aspect of the teaching methodology for the users was the fictional scenes of a hacker at work. This generated empathy with those fictional characters being attacked and insights into the techniques and motivations of the hacker. There was a clear sense that users strongly identified with the accidental vulnerabilities of those being targeted, as if it was themselves in that situation. This was clearly a powerful technique to trigger the 'need to learn' instinct in the user.

It was recognised early on that the tool needed to facilitate the user to create a Habit Change Action Plan. This is not easy to achieve in a short, self-directed learning session that was unsupervised. However, testing indicated that if the various options were presented to the student on how they might adopt different behaviours, it was considered valuable by the leaners to be offered an interactive way that they could prioritise these changes as if making 'pledges' to themselves. The developers saw genuine personal reflection by students when presented with this activity. This insight led to the production of an interactive sequence where users were asked to select specific behaviour change tokens and move them physically using their cursor onto a mobile phone screen image. This was carefully

designed to appear like they were loading Apps. Users were then offered a reward that consisted of an expert calculation of the decrease of their vulnerability if they were to keep to these promises. This reward to the user quickly became recognised as an important incentive in fulfilling the task.

The developer then created the tool targeted at graduate workers who used social networks heavily. The tool exposes the fictional hacker at work, whilst facilitating the learner through a process creating their own action plan. The initial trials are taking place in the university and large and small commercial businesses. The key learning outcomes of these trials so far reassert the critical requirements identified in the early stages.

Young learners in a workplace environment are easily distracted, so the fictional storytelling element of the tool is a vital means to achieve 'immersion' and empathy with the person involved in poor behavioural experience.

Learners need to be able to control the pace of their learning and the devices they want to learn on; so platform diversity, gaming-style navigation and 'pause & save' functionality is important

The balance of content in the tools is challenging to get right. Too much documentary video and the learner tends to not engage in the analysis within the narrative and resorts to 'watching TV' mode. Too many quizzes and text-based information and they begin to seek rewards, distractions or just get bored and try and cheat the game!

Raising awareness is not enough as a measurable outcome. In fact, with some learners interviewed after using the tool, the respondents stated that after experiencing the initial fictional scenario, they were more afraid of their inability to do anything than they were before. The developer mitigates this risk by following up the input experience immediately with a module that supports the user in producing their own positive action plan to minimise the risk.

Learners need to know how they are performing at regular intervals during the experience. The developer's Learning Management Software (LMS) is configured so that the learner can see their scores regularly and receive comparative data about their performance against the rest of their peer group. This can incentivise the enthusiasm for learning by itself. Of course, their managers or tutors can also receive this data and aggregate it to see how individuals are performing with their peer group or even between different departments or operational sites. This performance dashboard helps HR or Business Trainers to spot learning trends in their organisation and trigger additional support actions locally where necessary.

As the trials continue, further data and qualitative evidence will emerge that adds to the knowledge we have of how to migrate the student learning experience related to cyber security to the workplace.

VI. CONCLUSIONS

We would like to conclude by reflecting on our experiences to offer some general tips for those about to embark on teaching psychological principles to cybersecurity students.

As with all interdisciplinary teaching, materials need to be adapted effectively to provide appropriate links to the other discipline. In the case of cybersecurity, psychology materials need to be linked to topics taught on other units within the cybersecurity course and to show an awareness of the professional context of cybersecurity. It is important to deliver the materials at the correct level, taking into account the relevant intended learning outcomes and educational stage. At the 1st year of an undergraduate degree, the emphasis needs to be on practical activities and workshops can be used to demonstrate how recommendations based on Psychology can be put into practice. Indeed, examples can be used to illustrate where Psychology has *not* been considered to great effect! At final year undergraduate level, we found that students appreciate more detail as to *how* research was conducted and they need to develop skills to allow them to consider different psychological methods to evaluate the security of online systems. At post-graduate level, students are interested in hearing about ground-breaking research where psychology is being applied to inform cybersecurity, but also they appreciate discussing the philosophical debates. It is important not to overwhelm students (at any level) with psychological content but to provide case studies and references to support the concepts being covered. Similar to being prepared regarding the curriculum and educational level of your intended learners, some understanding of the profile of your intended learners can assist in developing Psychology materials for cybersecurity students. For example, the style of presentation of Psychology activities can be adapted to better match the approaches to studying of cybersecurity students.

Finally, it is important to recognise that students will have a certain perception of what Psychology covers. It is common for some cybersecurity students to think Psychology is only concerned with treating psychological disorders or that it is an 'un-scientific' way of explaining human behaviour. As a result, it is useful at the start of any contact with cybersecurity students to briefly cover what is Psychology and what is not Psychology and to differentiate between academic Psychology and 'popular' Psychology. This helps to contextualise the wider role of Psychologists in the many areas of modern life relating to computing and technology. This has been helped recently with programmes such as 'Hunted' employing forensic psychologists and cybersecurity experts to hunt escapees.

REFERENCES

[1] Tetri, P., & Vuorinen, J. Dissecting social engineering. Behaviour & Information Technology, 32(10), 2013, pp.1014-1023.

[2] Cialdini, R. B. Influence: Science and Practice (5th ed.). Englewood Cliffs, NJ: Prentice Hall, 2008.

[3] McAlaney, J., Thackray, H. and Taylor, J. The social psychology of cybersecurity. The Psychologist, 29 (9), 2016, pp.686-689.

[4] McGettrick, A. ACM Report 'Toward Curricular Guidelines for Cybersecurity' 2013. Accessed on 15/2/17 from https://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf

[5] Hamman, S.T., Hopkinson, K. M., Markham, R.L., Chaplik, A.M. & Metzler, G.E. Teaching game theory to improve adversarial thinking in cybersecurity students. IEEE Transactions on Education, 99, 2017, 1-7.

[6] Rogers, M. K. The psyche of cybercriminals: A psycho-social perspective. In G. Ghosh & E. Turrini (Eds.), Cybercrimes: A Multidisciplinary Analysis, 2010.

[7] Fullwood, C. The role of personality in online self-presentation. In A. Attrill (Ed.), Cyberpsychology, 2015, 9 - 28. Oxford: Oxford University Press.

[8] Taylor, J., & MacDonald, J. The effects of asynchronous computer-mediated group interaction on group processes. Social Science Computer Review, 20(3), 2002, pp.260-274.

[9] Johnson, D. Computer Ethics (1st edition). Englewood Cliffs, NJ: Prentice Hall, 1985.

[10] Johnson, D. Computer Ethics (4th edition). Englewood Cliffs, NJ: Prentice Hall, 2009.

[11] Dark, M. & Winstead, J. Using educational theory and moral psychology to inform the teaching of ethics in computing. Proceedings of the 2nd Annual Conference on Information Security Curriculum Development, Kennesaw, Georgia, 2005, pp.27-31. ACM Press: New York.

[12] Kohlberg, l. & Kramer, R. Continuities and discontinuities in childhood and adult moral development. Human Development, 12, 1969, pp.93-120.

[13] Greene, J & Hiadt, J. How (and where) does moral judgement work? Trends in Cognitive Science, 6(12), 2002, pp.517-523.

[14] Reese, H. W. The learning-by-doing principle. Behavioral Development Bulletin, 17(1), 2011, p.1.

[15] Richardson, J. T. E. Mature students in higher education: A literature survey on approaches to studying. Studies in Higher Education, 19(3), 1994, pp.309-325.

[16] Higher Education Statistical Agency. Qualifications obtained by students on HE courses at HEIs in the UK by level of qualification obtained, gender and subject area, 2012 to 2013, 2014. Accessed on 16/12/16 from https://www.hesa.ac.uk/data-and-analysis/publications/students-2012-13/introduction

[17] Halpern, D. F. Sex Differences in Cognitive Abilities, 2nd ed. Hillsdale, NJ: Erlbaum, 1992.

[18] Radford, J. & Holdstock, L. Gender differences in Higher Education aims between computing and psychology students. Research in Science and Technological Education, 13(2), 1995, pp. 163.

[19] Wilson, F. Can compute, won't compute: women's participation in the culture of computing. New Technology, Work and Employment, 18 (2), 2003, pp.127-142.

[20] Gibbs, J. C., Basinger, K. S., & Fuller, D. Moral maturity: Measuring the development of sociomoral reflection. Hillsdale, NJ :Erlbaum 1992.

[21] Layman, L., Cornwell, T. & Williams, L. Personality types, learning styles, and an agile approach to software engineering education. ACM SIGCSE Bulletin, Proceedings of the 37th SIGCSE technical symposium on Computer science education SIGCSE '06, 38(1), 2006, pp.428-432. ACM.

[22] Kolb, D.A. Learning styles and disciplinary differences, in: A.W. Chickering (Ed.) The Modern American College. San Francisco, LA: Jossey-Bass, 1981.

[23] Bandura, A. Social cognitive theory. In Paul A. M. Van Lange, A. W. Kruglanski, E. T. Higgins *(Eds)* Handbook of Social Psychological Theories, 2011, pp.349-373. Los Angeles, CA: Sage.

[24] Cyber Security Challenge UK, 2016. Accessed on 16/12/16 from https://cybersecuritychallenge.org.uk/