6th International Conference on Cybercrime Forensics Education & Training

Short Course Teaching of Cyber Security For Mid-Career Physical Security Professionals With Limited Academic Background

Chadwick D, Gan D, Loukas G, Frangiskatos D

C-SAFE Team, University of Greenwich, London, UK

cd02@gre.ac.uk

Keywords: Lifelong learning, cyber security, short course, teaching,

Abstract: This paper addresses the approach taken by the C-SAFE (Cyber - Security, Auditing, Forensics, Education) team at the University of Greenwich when asked to produce a one week course for physical security experts who wished to know more about cyber security technologies. This paper discusses the expectations of both teachers and learners and their resultant feelings after the course had been delivered.

Mature adults, returning to education for a short course, are liable to face various problems. They are not conversant with the academic approach and have been absent from formal learning for many years. They are required to learn a great deal in a short time when they have been learning ad-hoc on-the-job as they progressed through their careers. The academic detail of 'how and why' things happen contrasts with the accumulated practical on-the-job experience of simply making things happen.

The academic team itself also faced various problems. They lacked the practical everyday experiences of the students they were teaching, they were concerned about how to maintain the pace of learning with relatively 'novice' students, and how best to involve the students in the academic material especially as the students had varying background knowledge in cyber security technologies. Also, we discuss the problem of how to assess the students – what sort of assessment to give them, how to mark it, what kind of feedback to give etc.

A questionnaire was given to the students after the course delivery in order to explore their professional role, their expectations of the course and their suggestions for improvement. The students were given a graded assessment and asked about their feelings on their resultant marks – whether they did as well as they were expecting or otherwise. This has resulted in a set of useful guidelines for teaching short courses in cyber security to mature learners involved in lifelong learning to enhance their career progression and knowledge diversity.

1. THE STUDENTS AND THE STAFF

'*New technologies are constantly increasing the complexity of business information, while more sophisticated technology and processes are needed to manage it. Furthermore, that information is simultaneously more critical to the business and more susceptible to attack or abuse'* so states the Information Security Forum [ISF 2012] an independent , not-for-profit association of leading organisations from around the world. And they are not the only ones becoming concerned about

organisational unpreparedness with regards to cyber security; the private security companies, hitherto solely concerned with selling their software or hardware products, are now starting to highlight the need for personnel to be more involved: '*Employees are the first line of defence against physical and digital attack vectors and require appropriate training* [Trustwave 2012]

Consequently, there has, in the past year, ever since the publication of the Cyber Security Strategy by the UK government [Clemente D, 2011]**,** been an emphasis on new and improved training and education initiatives in the cyber security field. Many organisations have directly and indirectly warned of the need to take cyber security seriously and train personnel accordingly. Accordingly, in May 2012, the C-SAFE team at the University of Greenwich, were tasked with providing a short training course, no more than 5 days, to introduce physical security practitioners to a working knowledge of cyber security. Physical security practitioners are people such as police officers, private security professionals and other security experts dealing with such issues as protecting personnel, protecting physical assets, securing buildings and equipment, and ensuring that cash and credit cards were free from compromise. They were all mature persons, over 40, in managerial posts, and were primarily mid-career professionals looking to enhance their knowledge base and progress their careers. But, for most of them, it was many years since they had been 'students' in a formal academic setting such as a university; most had learned their skills on the job or through short hands-on, highly practical training courses and were unfamiliar with classroom and laboratory based teaching. However, they were all primarily from the same industry background and shared a common body of knowledge that they could all relate to.

The C-SAFE team reasoned that they would need to teach such topics as network and internet security, cyber attacks –what they were and how to prevent, detect, and mitigate them, pen-testing basics, principles of forensic investigations, and such management topics as IT security standards and policies. However, a number of issues presented immediately: what background in IT and digital concepts did these practitioners actually have, and what topics were they most needing to know about? Also, and most importantly, what was the best way to teach these older learners: how well would they take to formal academic education after being away for so long, how quickly could they learn new material, and how well would they relate to theoretical as well as practical demonstrations of security concepts? The teaching team realised that a positive attribute of the cohort was that they all shared a similar working experience of physical security matters and that this might be useful for providing reference points for the cyber topics helping them to learn from each other; however, the teaching team also realised that their own knowledge of physical security practicalities was limited.

The teaching team approached the task by comparing the new learners (security professionals) with their 'normal' HE students i.e. undergraduate and postgraduate students, who they were accustomed to teaching – see table 1. From this, the team became aware that these mature but specialised students would have particular needs. Several years prior to this, the Higher Education Funding Council for England had stated that lifelong learning requires '*novel approaches to further engage adults'* [HEFCE, 2004]. In addition, education journalists, in the respected news media, had often made a point that returners to education might be requiring special treatment:

"*We are trying to … produce students who …enjoy and do well when they get there (university) … to be re-inspired and re-excited by learning*" [Swain H, 2006]

	Security Professionals	'Normal' HE students
Prior Academic experience	Little academic exposure for many years	Extensive recent exposure to academia
Type of Learning: Formal v. Informal	Informal; learning ad-hoc on job, slowly over time – occasional short training	Formal; structured learning, intense, in formal setting
Prior Learning Type: Education v Training	Practical Training: Hands – on, make things happen	Education: Practical + Theoretical - How and why things happen
Prior IT Knowledge	Very limited	Usually extensive
Prior Industry Experience	Much experience , highly specific, homogenous	Little experience, highly diverse, heterogenous
Prior experience: Management roles	Extensive as all were mid-career mature individuals	Limited as mostly quite young with limited work experience

Table 1: Comparison Of Security Professionals With Normal HE Students

2. PROBLEMS ENCOUNTERED AND SOLUTIONS

2.1 Incorporating The Industry Experience of The Learners

Staff did not share the detailed industry experience of the students – so how best to relate to them? Much prior work was undertaken exploring security industry issues that may be pertinent e.g recent crimes, events or terrorist activities and various events were noted. Staff researched forthcoming topical events e.g. the visit of the Queen to Greenwich in April, and the visit of the Dalai Lama to London in May. Also researched were topical events such as recent crimes and attempted acts of terrorism as well as media-reported events involving hacking, ID theft etc. It was felt that this would create a common background that staff could share with the learners. It was also felt that allowing the learners to bring in events from their working lives during the teaching sessions would give them reference points to each other which would help them to bond as a group, socialise more easily, and learn from one another.

2.2 Handling the Learners' Return to Academic Learning

The teaching team were particularly concerned about how to get through all the material in the time and whether the pace and methods of learning might be too much for the cohort. A timetable was constructed consisting of relevant topics but with long blocks of lecturing broken up with tea/comfort breaks (lashings of tea/coffee and biscuits provided). During these refreshment breaks, and also during the lunch break, the teaching staff socialised with the learners and made themselves available to deal with individual issues with the material. At the same time, these breaks enabled staff to gain feedback on how well the learning was going. It was also agreed that lectures were to be interspersed with activity sessions and hands-on tutorials especially incorporating challenges and games e.g. in the encryption topic the students were asked to encrypt and decrypt various messages

in competition with each other. In addition, strong contacts were established with prominent personalities, people who exhibited some influence and respect within the cohort, somewhat akin to the 'connectors' described in Malcolm Gladwell's book 'The Tipping Point' [Gladwell M, 2002]. These 'connectors', once identified and befriended by the teaching staff, gave valuable feedback on how well things were going within the student cohort.

2.3 Content Choice for Learners With Diverse and Limited Prior IT Knowledge

An initial 'introductory' lecture was given to explore the IT knowledge of the cohort and their working backgrounds. The teaching staff really needed to know which subjects to concentrate on i.e what did the learning cohort really need to know for their jobs? But, more importantly, was to determine the preparedness of the cohort for learning sophisticated material that often assumed a modicum of background knowledge in IT. Occasionally, this lack of background knowledge surfaced in the classroom and the topic under discussion was inadvertently digressed into another area to resolve a fundamental concept. For instance, it was needed, at one point in the encryption session, to show how the binary stream of a simple message could be encrypted. A simple text message was shown and converted to ASCII ready for encryption. It quickly became evident that many students did not know what ASCII was. A quick detour to show the ASCII table and how an ASCII code was generated each time a keyboard key was pressed only broadened the discussion further. Some students began asking 'what if you were in Russia' so the discussion digressed into 'character-sets' and then one asked 'what about in China – what alphabet do they use?' The discussion concerning ASCII took up approximately 15minutes of class time although ASCII itself was really just an incidental topic to the main topic of encryption. Again, socially meeting the cohort during breaks gave valuable and surprising feedback; many reported that the short discussion on ASCII had filled in many gaps in their existing knowledge of how computers worked and they were grateful that it had been covered - one student even went so far to say it was the most important thing he had learned so far (on the second day)!

2.4 Choosing The Type Of Assessment

A definite problem for the teaching team was to decide on the nature of the exercise to give the cohort as part of their assessment and a number of criteria were discussed within the team as the teaching progressed. Firstly, it was reasoned that, as many of the students were attending to enhance their careers, a real-world practical exercise of some kind was needed rather than a classroom based exercise involving solely bookwork. Secondly, that as the cohort had much prior experience in physical security then an exercise incorporating this aspect might catch their imagination and encourage them to get equally as involved in the cyber issues. Lastly, the exercise had to have an element of urgency or significance with regard to contemporary events such as terrorism or crime to make it realistic. It was eventually decided to capitalise on a forthcoming visit of the Queen to open the recently refurbished Cutty Sark clipper-ship tourist attraction. As part of the assessment scenario, it was suggested that Her Majesty would also be visiting the university and that details of her visit might be held on the computer systems there – computer systems that could be open to compromise and attack from outside. The assessment exercise therefore involved the students in a complete security assessment of the University of Greenwich site, including the cyber aspects, as if they were being employed to do it for real.

The assessment was very successful; it was well done and there was strong evidence that the students were incorporating the recently learned cyber security material into their existing methods, rules and habits of professional conduct.

3. RESEARCH METHODS FOR ASSESSING THE TEACHING APPROACH

The team decided on several methods of assessing their teaching approach; a questionnaire for the students to complete anonymously, the lecturers' personal observation during the teaching, the actual content of the students' completed assessments, and the ad-hoc interviewing of selected learners (connectors). These four methods of enquiry are approved methods of social science and educational enquiry according to the literature [Creswell J.W. 2007]. However, the questionnaire was considered to be the main source of primary research data and was put together using principles from the British Educational Research Association [BERA 2010]. The full questionnaire is shown in Appendix 1 and the results are shown in Table 2. Overall, feedback from the learners was very informative. It was mostly positive and highlighted the areas the team most had to concentrate on in future deliveries of the course.

QUESTIONS		**REPLIES**	
Why sign up for course?	Employer sent me: 40%	Chose to come to enhance career:40%	Make UK safer: 20%
Prior knowledge requirement:	Right level: 40%	Required too much in a few areas: 60%	
Feelings about content	Neutral:20%	Good: 60%	Excellent: 20%
How can content be improved?	More pre-reads: 40%	More practical: 20%	No reply:40%
Course organisation?	Good: 40%	Excellent: 60%	
Presentation:	Good: 20%	Excellent: 80%	
Best things about course:	No reply: 20%	Liked the staff: 60%	Nice biscuits: 20%
What aspects need to be changed?	Too much assumed knowledge: 40%	No reply: 60%	

Table 2: Answers to End-of-Course Feedback Questionnaire in Appendix 1.

4. GUIDELINES FOR FUTURE SHORT COURSE TEACHING: THE CSAFE APPROACH

Based upon the questionnaire feedback, the lecturers' experiences in the classroom, the students' assessment, and verbal feedback from some of the students, the team identified five areas of importance in teaching adult learners.

Content factors: what topics should be taught
Social factors: how staff should relate to the learners
Advance (Prior) Learning: what pre-reading or introductory sessions were needed
Feedback : what feedback was to be sought and from where/whom?
Experience: what common work-related experiences did the cohort have?

4.1 Content Factors

What topics should be taught? This needs careful thought as the teaching staff should be sure that what they wish to teach is what the learners really need to know. One of the topics included in the original course at Greenwich was 'Security Policies'; the staff considered this to be an important issue that all the learners would want to know. However, the feedback from the social events and connectors indicated that this was the least attractive of all the topics taught as the learners felt that they already knew this material. Another topic that missed the target was Social Engineering. It transpired that the learners already had substantial knowledge of this issue in general terms and found the lecture quite boring until phishing was introduced which was the cyber aspect that was not so well understood. It was decided for the next occurrence to omit general discussion of social engineering and concentrate only on the cyber aspects.

4.2 Social factors

Social factors were identified early on as being of utmost importance. The 'normal' didactic and sometimes hierarchical approach to education where the lecturer is somewhat aloof, highly pedagogic (or maybe demagogic) and teaches from the front from a position of utmost authority does not fit well with mature learners who have achieved some distinction in their own fields. It seems a 'let's learn from each other' approach works much better because it acknowledges the learner's existing body of knowledge, their age and personal maturity, their management background, and that, in some instances, they really do know more than the lecturer. Such, learner-teacher relationships were identified by the staff as being critical and this finding was reinforced in the academic literature: Prosser and Trigwell [Prosser M & Trigwell K, 1999] discuss such relationships at great length and posit that prior experience of education is often rooted in highly formal lecturer-student relationships which maintain an intellectual and social distance between the two parties and that this is not always beneficial for the learner. The teaching team, therefore, were particularly concerned not to make the learners feel inadequate in any way.

4.3 Advance (prior) Learning Requirements

This is perhaps where the Greenwich team were at their weakest. Mature learners come with such diverse basic knowledge that they need a base-line to show where they should all be starting from. Although basic explanations can be given as and when they arise this can seriously impede the flow of learning of the current topic. Also, too many 'basics' occurring too quickly one after the other can cause students to become overloaded and confused. There is a definite need for pre-reading to be given before the course begins, not only as a preparation beforehand but also as a source of reference during the course teaching. There is also a requirement on the staff to arrange the taught topics such that basics taught in one topic are not then covered a second time when they arise in a later topic and that topics, as far as is possible, build upon each other. Lecturers need to cooperate in this handling of basic issues and recurring topics as evidenced by the literature:

'Teachers need to collaborate in order to define and implement programmes. There must be progression – vertical connections and coherence- and horizontal connections within the specialist areas …' [Bourdieu P, 1999]

4.4 Feedback

This was found to be one of the most important features. The use of social breaks during the day and social events during the evening in which the staff could meet and talk freely with learners was a rich source of feedback. Building relationships with 'connectors' in the student cohort was, also, very useful. Both of these sources enabled ongoing feedback to be analysed and acted upon as the course progressed. On one occasion, a lecturer completely rewrote a lecture based on his feedback from the previous day.

4.5 Experience

In his book, *Teaching Adults,* Alan Rogers states *"Adult learners should not be divorced from their background if their learning is to be effective"* [Rogers A; 2002]. Rogers' statement is very true. The teaching staff found that relating to the existing knowledge base of the learners was the best way to establish rapport, understanding and common ground for discussion. An example of this was the assessment exercise based on the Queen's imminent visit to Greenwich and how they, as physical security practitioners, might prepare for this. Once the students had become involved, they were asked to explore any cyber issues that also might have arisen. This approach was well received as they were able to use much of their existing professionalism in dealing with the, to them, newer aspects of cyber security.

5. CONCLUSION

This was a valuable learning experience for all involved. The short course was judged by the students to have been a success despite their feedback misgivings and the general consensus was that it should be repeated in the future with new cohorts of students.

But why should we be so concerned about the training and education of mid-career professionals in cyber security topics? David Blunkett MP , the former Home Secretary (Blunkett D, 2011) who was an invited speaker at the Cyber Security 2011 Conference in London, gave a speech in which he outlined the need for three areas of research and expenditure to meet the UK governments 2011 cyber security initiative (Clemente D, 2011). David recognised three goals; (1) to teach schoolchildren and the public to be security aware when using the internet, (2) to bring existing security professionals up to date in the growing field of cyber security, and (3) to perform leading edge research into cyber-attacks, technologies, and defences. The Greenwich C-SAFE team believe that their latest course, tailored specifically for physical security specialists, goes some way in meeting David Blunkett's second goal.

In addition, in the follow-up conference in July 2012, James Quinault, director of the Office of Cyber Security & Information Assurance in the Cabinet Office (a branch of the UK government) has stated that the strategy objectives of the UK government in terms of cyber security are Resilience, Awareness, Skills & Capabilities [Quinault J, 2012]. There is no doubt that updating the skills and capabilities of physical security practitioners to include cyber security awareness is pertinent to this political objective.

It is believed the CSAFE approach to providing short courses for existing security personnel, herein described, takes into account the problems of teaching older, more mature, learners who have a substantial body of knowledge already in existence.

References

BERA 2010; - website of British Educational Research Association,

http://www.bera.ac.uk/questionnaires/questionnaires-basic-principles accessed on 14 June 2010

Blunkett D, 2011; *UK Cyber Security Strategy*; Speech by David Blunkett (Rt. Hon, UK MP, Former Home Secretary) Invited Speaker at Cyber Security 2011 Conference, QE11 Conference Centre, London, UK, 29 Nov 2011

Bourdieu P. 1999; Principles for Reflecting On The Curriculum (a summary from Moon B., & Murphy P., "Curriculum In Context", Paul Chapman Publishing 1999, pp245-252)

Creswell J.W. ; 2007 : *Qualitative Enquiry & Design – Choosing Among Five Approaches*; Sage Publications 2007

Clemente D, 2011; *The UK Government Today released its 2011Cyber Security Strategy*. International Security Programme, Chatham House, UK, 25 Nov 2011: http://www.bbc.co.uk/news/technology-15893773

Gladwell, M, 2002; *Tipping Point: How Little Things Can Make a Big Difference*; ISBN: 0-316-31696-2

HEFCE Circular Letter, 2004; *Lifelong Learning Networks (LLNs)* : Higher Education Funding Council for England http://www.hefce.ac.uk/aboutus/sis/ accessed on 14June2010

ISF 2011; *Information Security Governance: Raising the Game*; Informational document ISF 11 ISG (Marketing) 2011; Information Security Forum Limited

Prosser M, Trigwell K, 1999; *Understanding Learning and Teaching: the Experience in Higher Education*; Open University Press; 1999

Quinault J, 2012; Director of the Office of Cyber Security & Information Assurance in the Cabinet Office, Invited Speaker at National Security 2012 Conference, QE11 Conference Centre, London, UK 3rd July 2012

Rogers A, 2002; *Teaching Adults*, 3rd Edition, Open University Press, 2002

Swain H; *Fast Forward To The Past*; Education Guardian Sept 26 2006 quoting Kevin Stannard of Cambridge International Examinations.

Trustwave 2012; *Information Security Strategy Pyramid for 2012*, Trustwave 2012 Global Security Report, Informational Publication of Trustwave Holdings Inc, 70 West Madison Street, Chicago, USA

Bibliography

Armitage A, et al 2007; Teaching and Training in Post-compulsory Education; Open University Press 2007

Gravells A, 2008; Planning and Enabling Learning in the Lifelong Learning Sector ; 2nd Edition, Learning Matters Ltd 2008

Wallace S, 2007; Teaching, Tutoring and Training in the Lifelong Learning Sector; Learning Matters Ltd, 2007

Appendix 1

The Questionnaire

Why did you sign up for the course?
The course assumed you had some relevant prior knowledge before starting . Which best describes your feelings about the prior knowledge that it assumed?
What do you feel about the overall content of the course? a) Very good ____ b) Quite good ____ c) Neutral ____ d) Not good ____ e) Very poor ____
Any ideas about how the content of the course could be improved?
What do you feel about the way the course was organised? f) Very good ____ g) Quite good ____ h) Neutral ____ i) Not good ____ j) Very poor ____
What do you feel about the overall presentation of the course? a) Very good ____ b) Quite good ____ c) Neutral ____ d) Not good ____ e) Very poor ____
What were the three BEST things about the course? 1. 2. 3
What were the three aspects of the course most in need of change? 1. 2. 3
Do you think the course was good value for money? a) Very good ____ b) Quite good ____ c) Neutral ____ d) Not good ____ e) Very poor ____