**Delivering Cybersecurity Education Effectively**

**Draft Chapter**

**Introduction**

This chapter draws on current research and best practice into teaching in cybersecurity in higher education. The chapter provides a theoretical and pedagogical foundation for helping tutors make decisions about what topics to include (detail provided in previous chapters) and approaches to teaching and assessing the cybersecurity curriculum. There are of course a range of potential stakeholders in cybersecurity education ranging from government, policy and law makers to all members of society. However, for the purposes of brevity this chapter will focus on learners and those creating and delivering cybersecurity education in the Higher Education sector.

The chapter will discuss the opportunities for different and innovative ways of learning about cybersecurity – designed to provide deep learning and thus a greater understanding of principles, theories and applications of cybersecurity.

In recent years, computing technology and computer systems have experienced dramatic growth. The growth in the number of systems (communications, information systems, Internet systems and e-commerce) and the advances in the scale, the functionality and the usability of systems have provided opportunities for malicious users to exploit insecure and non-robust systems. The pace at which companies and their customers have embraced technologies such as cloud computing, smart things, mobile things, and the Internet of Things (IoT) has created an environment that is changing faster than organisations and legislators can keep abreast of. It’s not only systems that are changing – the way people use the systems and the expectations of speed and convenience means that cybersecurity can often be relegated in importance. Allied to the growth in systems technologies is the growth in the amount of data that is provided and the huge variety of ways in which data is collected, manipulated and stored.

The range of systems and technologies and the speed of implementation and adoption provide opportunities for cybercriminals to exploit. In addition to chance to take advantage of vulnerabilities in systems the advances in technology give computer criminals the opportunity to conceal their activities, to cover their tracks and attempt to destroy evidence of their actions. The ability to prevent cybercrime attacks and cybersecurity breaches that have taken place and the resultant requirement to examine the cybertrail have raised the need to develop specialists in cybersecurity – a set of practitioners who have the methods, skills and techniques to prevent, detect, recover and restore systems and data in the event of an attack.

The global news headlines frequently present cybersecurity attacks, vulnerabilities or failures, illustrating that there is an increasing loss of control over the cyber-threats to business. Recent years have seen high profile attacks to major corporations such as Tesco Bank, Talk Talk, Daimler Chrysler. In 2017 the NHS in the UK (along with 160 other organisations) were rocked by the “wannacry” attack. Other headlines have reported belief and fear that the recent U.S. elections could be manipulated by a foreign power and speculation over whether development in artificial intelligence could lead to cyber attacks perpetrated by machines, without any human motivation.

The changing technology environment and the growth in threats and potential threats means that the role of cybersecurity is increasing in importance. As society and business becomes more reliant on cybersecurity the efficiency of cybersecurity education – what we teach and how we teach it – becomes an important objective. Similarly we need to consider the learners, what they need and want to learn as well as how they learn as in integral part of cybersecurity education.

McGettrick (2013) argues for the need for cybersecurity education as opposed to cybersecurity training. In this chapter the focus will be on cybersecurity education – but as tends to be the case with discussion on any aspect of cybersecurity there is overlap between the categories, so some aspects of training will come in to the consideration of cybersecurity education. Part of the rationale for looking at this topic is because there are so many different providers offering a range of different cybersecurity learning products claiming to deliver education and training. We will return to this later in the chapter.

It is worth asking the question as to why there should be consideration given to examining the ways in which to deliver cybersecurity education. Cybersecurity is a complex and wide-ranging topic (or series of topics) to consider. The complexity associated with cybcersecurity means that there is a need to consider different teaching approaches to enable cybersecurity learning. There are many topic domains in which we potentially have interest in cybersecurity including (but not limited to) information security, systems security, network security and Internet security each with a set of fundamentals and principles and different theories and applications. The breadth of subjects to include makes the delivery of cybersecurity education even more complex.

Teaching cybersecurity as a subject in its own right is complicated enough. However, there is a further complicating factor because there is an additional expectation that cybersecurity is taught as part of the curriculum across the computing / computer science family of disciplines. Irons et al (2016) argue that embedding cybersecurity into computing science degrees presents a real opportunity to ensure that everyone involved in creating the digital economy – especially the technology underpinning it – understand the threats, vulnerabilities and mitigations that need to be managed. Cybersecurity has recently (2017) been added to the components of the BCS accreditation criteria, reflecting the importance placed on cybersecurity and the expectation that all computing graduates should have knowledge and skills in cybersecurity as they move towards chartered status.

Cybersecurity is a rapidly changing and rapidly evolving discipline. This means that anyone involved in cybersecurity to a greater or lesser extent, from a technical to a managerial, from an organisational to an individual level needs to constantly review and update their knowledge on cybersecurity. This in itself presents a challenge for efficient cybersecurity education.

Anyone working or seeking to work in cybersecurity needs to develop a range of abilities and competencies in addition their technical knowledge of cybersecurity. For example cybersecurity practitioners will come across situations where they are required as professionals to be able to make judgments when faced with uncertainty. Linked to this is the need to be able to have the confidence to react quickly to situations with robust and reliable solutions. Cybersecurity practitioners will need to be able to work both as part of a team and independently. Teaching these competences has an impact on the way that we seek to teach cybersecurity efficiently and effectively.

Invariably when we look how to teach cybersecurity education effectively there will be consideration given to the topics covered elsewhere in this book. Where appropriate there will be cross-reference to materials and topics covered in sections 2 and 3 of this book. In particular we will look at the links between the other chapters in section 3, curricula, body of knowledge and education programme.

In the remainder of this chapter we will cover the challenges in cybersecurity education; what to teach; how to teach effectively; approaches to learning and teaching cybersecurity; balance between theory and practice; use of technology in teaching; assessing cybersecurity knowledge, understanding and skills; and the need for continued professional development.

**Challenges in Cybersecurity Education**

There are many challenges in cybersecurity education and these will be discussed in this section. Understanding and overcoming the challenges in education will enable cybersecurity education to be delivered effectively. This section will look at the particular challenges in cybersecurity education and compare to the approaches used in other computing disciplines.

One of the key challenges in cybersecurity education is addressing the skills gap. (ISC)2 report (2016) suggest that there are 350,000 open / unfilled cybersecurity positions unfilled worldwide and that this number is growing. Oltsik (2017) suggests that the skills gap in cybersecurity is getting worse. Oltsik identifies a growing problem with organisations indicating more than a doubling of “problematic shortage” of cybersecurity staff, increasing from 23% in 2014 to 51% in 2018. This provides a real challenge for cybesecurity educators.

The objectives of the cybersecurity education will depend on the level of learning to be achieved, the previous experience and knowledge of the participants, the subjects and topics of interest to the participants and the desired learning outcomes from the education. There are many challenges in cybersecurity education, as we shall see later in this chapter. However, the range of people potentially interested in cybersecurity and the variability in the depth and breadth of cybersecurity knowledge that they have, and that they need, mean the cybersecurity educators can be called on to provide a wide variety of educational experiences.

The National Cyber Security Centre (NCSC) have produced a cyber attack categorisation framework (2018) designed to indicate the priority that should be given to investigating different cyber attacks. The new framework increases the number of classifications from three to six (category 1 ‘national cyber emergency’ to category 6 ‘localised incident’. Whilst the framework is designed to improve consistency around response and provide a better outcome for victims, the framework also illustrates the complexity of the cybercrime environment. The complexity can also be seen in the need for cybersecurity education – ranging from a general awareness that cybersecurity is a potential threat, through to what the threats are to what can be done about cybersecurity at a personal level to in depth technical expertise in creating and implementing cybersecurity infrastructure.

It is not the intention in this chapter to provide a framework on which topics to cover at which level – suggestions have been recommended in the previous chapters in this book. Harris and Patten (2015) provide a very good discussion relating cybersecurity skills and knowledge to levels of learning, linking cybersecurity to Bloom’s and Webb’s taxonomies. The ACM/IEEE (2017) report suggests a series of expectations for the cybersecurity curriculum and recommends which cybersecurity topics to consider. A common theme from all those who examine and evaluate the cybersecurity curriculum is the progression from remembering and understanding the cybersecurity fundamental principles and theories, to applying the principles and theories to cybersecurity problems, to making judgements based on those principles (and on standards and legislation) to creating solutions and providing strategic direction for cybersecurity.

This has a direct bearing on the way we teach cybersecurity. In particular we need to consider different ways of teaching for different aspects of the curriculum and using appropriate approaches to contextualise the expected learning for students and learners.

A further challenge in cybersecurity teaching is the interdisciplinary / multi-disciplinary nature of cybersecurity. Whilst there are a range of diverse discipline including criminology, psychology, sociology, law and mathematics which inform a range of cybersecurity topics including policy, human factors, ethics, and risk management, cybersecurity remains fundamentally a computing-based discipline. The challenge in teaching cybersecurity is that cybersecurity is both informed by the interdisciplinary content, and driven by the needs and perspectives of the computing disciplines that provide the underpinning fundamentals of cybersecurity.

The multi-disciplinary aspect of cybersecurity is not necessarily a benefit – it could be argued that the multi-disciplinary aspects potentially dilute the core of the subject. However, it is suggested in this chapter that drawing from other disciplines strengthens cybersecurity in terms of rigour and robustness and also strengthens the suggestion that cybersecurity can stand as a separate and distinct discipline in its own right.

In order to allow students to apply theory and develop cybersecurity skills there is a need to analyse appropriately complex case studies and problems. The challenge for teachers is to develop materials that allow problem solving, analysis and application of theory and at the same time provide an environment to practice and make mistakes without falling foul of regulations (for example JANet regulations in universities in the UK) and to protect students and learners from exposure to inappropriate cases.

In any cybersecurity problems in the real world there are many complex and inter-related variables to consider, a number of legal considerations to contend with, many technical issues to be aware of and many cybersecurity principles, theories and guidelines to apply. There is a challenge for cybersecurity educators to put over this complex environment in teaching the subject without overwhelming students.

**What to teach ?**

The curricula and body of knowledge of knowledge have been covered previously in chapters, 9, 10 and 11 of this book. In addition the material covered in this book as part of the National Cyber Security Strategy (2017), the Cyber Security Body of Knowledge (CyBOK) project has been established to codify the foundational and generally recognized knowledge on cybersecurity. At the time of writing the first two Knowledge Areas – Cryptography and Software Security – are open for public consultation. They can be viewed at [www.cybok.org](https://cas-01.uni.ad.sunderland.ac.uk/owa/redir.aspx?C=oiAnhql-1IhI7kN6RCcmt7QVy4zsNKRFEffcy1QslrTYpQayjt_VCA..&URL=http%3a%2f%2fwww.cybok.org). The ACM have provided a comprehensive document outlining the ccurriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (2017).

In this chapter we will explore what to teach about cybersecurity depending on the audience of learners and the relationship to how to deliver cybersecurity education effectively. What to teach and how to teach it effectively will vary depending on the audience and the experience of those in the audience. There is a large spectrum of potentially interested learners ranging from school pupils (all pupils), through school pupils studying computing and computer science at GCSE and A – level to students at college and university (again with a split between cybersecurity specialists, to computer science students to students in other disciplines such as business and engineering) and on to practitioners and professionals requiring continued professional development (CPD).

In this chapter we focus on cybersecurity education as opposed to cybersecurity training. The difference between training and education is illustrated below using Yasinsac et al’s (2003) suggested classifications.

|  |  |
| --- | --- |
| **TRAINING** | **EDUCATION** |
| Skills | Knowledge |
| Application | Abstraction |
| Using tools | Developing tools |
| Applying procedures | Establishing procedures |
| Practice | Theory |

Although in order to develop proficiency in cybersecurity there needs to be a balance between the theoretical and conceptual knowledge essential to understanding cybersecurity, and the practical skills that support the application of that knowledge.

As indicated earlier in the chapter cybersecurity practitioners will come across situations where they are required as professionals deal confidently with uncertainty and make judgments about complex situations. One of the ways to address the potential issues of judgement and confidence is to consider computer ethics in the context of cybersecurity.

There is a significant challenge in teaching ethical awareness and embedding ethical principles into the cybersecurity teaching. There is a need to make students aware of the potential for misuse of cybersecurity tools and techniques as well as the need to instil ethical and professional behaviour into cybersecurity practices. The teaching of computer ethics is normally embedded throughout computer science programmes in order to meet professional body (for example BCS) expectations and requirements. Teaching cybersecurity requires emphasis on ethical issues early in the curriculum in order to instil the importance of appropriate ethical behaviour right at the beginning of the students' cybersecurity programme so that they have the ethical tools and mind set to allow them to deal with complex and challenging ethical dilemmas faced in cybersecurity education.

The coverage of computer ethics focuses on the professional responsibilities of a cybersecurity practitioner, namely using the skills and techniques of cybersecurity professional to the benefit of society and not to use cybersecurity knowledge for criminal activity or personal gain. A further thread of ethical consideration is to deal with cases sensitively and professionally maintaining the confidentiality and anonymity of participants in case or problem being studied.

There is also a “gamekeepers and poachers” dilemma in teaching cybersecurity. In order to develop the skills and techniques required to become a cybersecurity practitioner, students need to develop understanding and knowledge of the tools and techniques applied by cyber criminals. As students realise the security vulnerabilities and weaknesses in procedures and systems the temptation to utilise this awareness may arise. The concern in the “gamekeeper poacher dilemma” is that universities could become complicit in creating cyber criminals of the future rather than developing practitioners who are motivated to work against cyber crime.

There is potentially a different type of ethical dilemma associated with the teaching of cybersecurity, namely cybersecurity has the potential to put forward an unbalanced view and perspective in tackling computer crime, cyber attacks and misuse of data. One way to redress this potential concern is to include topics such as civil liberties and the Human Rights Act (1998) in the ethical consideration of cybersecurity.

**Delivering Education Effectively**

In this section we will present a brief discussion on what we mean by delivering education effectively – looking at engagement of learners, how learners learn, getting the learning materials and concepts to learners and metrics how to evaluate effectiveness of learning. These topics will be explored in the cybersecurity context.

In order to provide effective teaching in cybersecurity there is an expectation that the lecturer has a level of expertise and understanding of the subject, knows how the students learn and understands the range of pedagogic approaches that can be utilisied. Subject knowledge is required to enable the lecturer to determine the most appropriate way to put across the subject and to organise and structure the teaching activities (and the series of learning activities if appropriate) in such a way that enables students to learn. In order for teaching to be effective it is important that the lecturer understands the level that students are at in their learning and us such appreciate what it is students know. Understanding the audience of learners will help the lecturer to identify the most appropriate approach to ensure clear communication and to determine the best ways to stimulate, inspire and excite the students.

As well will see with all the methods discuss in the next section, effective teaching is not only dependent on good lecturers and good lecturing. There is a responsibility on students to engage with the learning opportunities afforded them. One way to male teaching more effective is to work with students so that they understand their role in learning.

It is important for providers of cybersecurity education to consider the effectiveness of the learning opportunities to enable students develop the wide range of skills needed to be a cybersecurity professional. As well as the theoretical knowledge and technical skills involved in cybersecurity as a subject there is the need for cybersecurity professionals to have expertise in team working, the ability to make judgments (often under pressure) and the capability to become life long learners.

It is all well and good looking to have effective education, and of course we are interested in effective cybersecurity education. What do we mean by effective education and how do we know when cybersecurity education is effective ? Effective education can be viewed from a number of perspectives and different stakeholders will have different views on effectiveness. Suffice to say is that we need to measure something – but what ??

In this chapter we are interested in what makes effective cybersecurity education from a student perspective, but first we will consider what might be a suitable metric to use in determining whether the cybersecurity education is effective.

It has long been acknowledged (Lundstedt, 1966) that it is difficult to quantify what we mean be effective teaching. Quantifying effective teaching remains problematic today – there is an acceptance that effectiveness relates to the communication between teacher and learner, but that there is also an understanding of the learner needs in making teaching effective. Recently there has been a move towards considering “value” and “value added” in considering effective teaching. The concepts of “value” and “value added” are particularly relevant in considering effective teaching in cybersecurity.

There are of course a range of perspectives on what constitutes effective teaching. From a government perspective there is a desire to drive down the cost of teaching in Higher Education and at the same time improve quality assurance, which gives an interesting dilemma for providers of Higher Education. Linked to cost, effectiveness might be measured in terms of class size, or the amount of contact time – it will depend what is important for the education provider.

Since the introduction of the National Student Survey (NSS) in the UK there has been an increasing emphasis on measuring student satisfaction and using student satisfaction as a proxy for effective teaching. There has been a significant amount of debate as the veracity of student satisfaction as a measure of effective teaching (for example Williams and Cappuccini-Ansfield, 2007), but whether we agree or not, the NSS remains a metric which is utilised by Higher Education managers, government and creators of league tables !

Other drivers as far as measuring effectiveness of teaching in HE focus on research, research outputs and research income. Putting an emphasis on research in cybersecurity might conflict with providing effective teaching. However, if we embrace the principles of the teaching research nexus (Jenkins and Healy, 2005) then embedding current research, developing students’ skills as researchers, and applying research informed teaching we can benefit the students’ learning experience.

Looking at efficiency in cybersecurity teaching from a pedagogic perspective the purpose is not have passive, compliant, surface learners in cybersecurity but to have participants who are independent, active learners who will be equipped with higher level skills in cybersecurity. In structuring our learning and teaching activities (discussed in the next section) it is important that think about how to ensure that we are developing higher skills and encouraging learners to be independent and active. This links in to key questions on learning and teaching in cybersecurity:

* What do we want the students to learn (linked to curriculum and syllabus – see earlier chapters in this book) ?
* What are the students actually learning (and how we measure a level of understanding) ? The measurement of actual learning will be returned to in the ways in which we assess student understanding in cybersecurity later in this chapter).

If we look at effective teaching and learning from a student perspective (it is suggested in this chapter that this is the most important perspective) then other variables come in to play. According to Cohen (1981) students want “systematic, stimulating and caring teaching that leads to success”. In order to achieve this in cybersecurity is it suggested that learning providers try to ensure that:

* learning is transparent;
* teaching activities facilitate dialogue between teachers and learners and between learners; and
* we develop communities of learners.

The next section will examine tools and techniques for the delivery of cybersecurity teaching taking into account the aspiration and expectation that the teaching is effective.

**Approaches to learning and teaching cybersecurity**

In this section of the chapter we will examine a range of alternatives to enable learning in cybersecurity and encourage learner engagement, and effectiveness of the learning opportunity. The different methods are not presented in any ranked order. The most appropriate method of delivery will depend on the subject matter and topic of cybersecurity, the level of cybersecurity experience of the learners and other variables such as group size and learning environment.

We will look at the benefits and issues associated with each approach. Each method will be discussed in the context of teaching cybersecurity and how they can enhance efficiency in the teaching of cybersecurity. We will also consider where and how online learning and educational technology can be utilised to enhance the efficiency of the particular method.

*Lectures*

There is place for lecturing as a didactic learning method in cybersecurity, especially in situations where the audience is very new to cybersecurity or the speaker is particularly inspiring. Experienced cybersecurity practitioners are able to share real life examples or “war stories” which can be very beneficial in contextualising cybersecurity theories, principles and issues for learners. Covill (2011) suggests that “students in a lecture-style class report learning a great deal, being involved in the learning process, and engaging in independent thinking and problem solving”. Lectures continue to be a dominant form of teaching in Higher Education in the UK, despite the assertion lectures are not always the most effective way of engaging students. The learning that takes place as a result if a lecture depends on student engagement, the relevance of the subject matter and on the abilities and style of the lecturer.

Research carried out by Irons and Devlin (2012) on inspiring teaching identified (form a student perspective) what student considered to be important in lecture sessions and perhaps more importantly what they did not like in lecture sessions. The following list indicated what students didn’t want from lectures or what they didn’t like about lectures:

* Endless amounts of facts being dictated for long periods of time;
* Just reading from slides;
* Someone who is unprepared and uninspired by the subject they’re teaching;
* Monotone, too many detailed slides, when the teacher is not interested in either the subject or the students’ understanding;
* Boring;
* Teachers who talk down to you and treat you like you’re back in secondary school;
* Too much information for 1 hour and we leave without complete understanding;
* When the teacher doesn’t want to be there.

The detail provided by students on what the found to be uninspiring is a really useful list of things to avoid when lecturing on cybersecurity.

The following list suggests what make efficient lectures from a student perspective;

* Whenever someone gets up and is enthusiastic about what they’re trying to teach you;
* When a teacher is comfortable enough about a subject to use examples of when they got it horribly wrong to help understanding;
* Yes – they’re very knowledgeable and willing to help all of the time;
* They make jokes or use funny real life situations;
* Use of stories or comparisons to help us learn;
* Their outlook and way of talking about things – friendly and approachable;
* Instead of just throwing information at you they got you involved in the subject;
* Passionate;
* They enjoy what they do;
* The way they delivered it – asked questions rather than giving answers;
* Their ability to make the subject relevant; and
* They broke down information into smaller more manageable sections.

The list of factors that appear to inspire students pertain to lecturing in cybersecurity. As well as the expectation of through subject knowledge it is important for those lecturing in cybersecurity to be enthusiastic, passionate and care about the subject matter. In many ways we are fortunate because of the subject matter and the relevance and currency of so many of the issues in cyber security and cybersecurity breaches. To this end, although it is a set of circumstances we would seek to avoid and prevent, the fact that there are so many news stories about cybersecurity, breaches of security, cyber attacks and cybercrime mean that we can relate current affairs to the theories and principles we are trying to convey in our lectures.

We can also enhance our lectures by use of technology – for example giving students access to lecture notes before hand on virtual learning environments (VLEs) or by using lecture capture technology so that students can access materials outside the lecture session.

*Flipped classroom*

The flipped classroom is an interesting way of changing the dynamic of lecture sessions. In a flipped learning session the students have access to the planned material in advance, undertake learning before they come to the classroom and then use the class contact time to ask questions, discuss issues and explore the subject in more detail. Exponents of the flipped classroom (from example Alvarez, 2011, Johnston and Karafotias, 2016) suggest that this is an effective way to use student contact time for effective learning.

The author has used this approach in cybersecurity teaching and has had mixed results. When students engage in the process and come to the class prepared (having done the homework in advance of the class) then the teaching sessions can be very productive – in particular when students are willing to ask questions and to debate and discuss issues and principles the learning can be really exciting. From a teaching perspective it is important to a) be well prepared for a range of topics to be discussed (often not the ones that were expected) and b) to have a plan B when students haven’t done the pre- work.

*Webinars*

Related to lectures in many ways, making use of technology, and much used in the cybersecurity subject area are webinars. Webinars enable those delivering sessions to deliver presentations to larger, geographically dispersed audiences. Webinars are live web-based video conference that use the internet to connect those hosting the webinar to the audience. The audience is not constrained by geography. Webinars are flexible in what is presented – audio, video, slideshows, demonstrations and can have multiple presenters from different locations. Some commentators, for example Joshi et al (2011) indicate that webinars are effective with “the most notable aspect of webinars was that it brought about the comparable gain in knowledge, skills and satisfaction”.

Webinars and the technology supporting webinars enable a number of learning opportunities which contribute to their effectiveness. For example, webinars have the following features, including:

* the ability to record the webinar – which (like lecture capture) allows the material to be reviewed at a later date and re-used by the learner;
* the opportunity to enable chat features which allows students to type in questions and queries without disturbing the flow of the session. Chat questions can then be addressed later;
* application sharing, where appropriate – allowing lecturers to share their desktops or applications, etc to help the audience get a better understanding of the topic;
* the capacity to conduct opinion polls – by using this at strategic points in the webinar the lecturer can conduct polls and surveys for the audience, which helps in terms of getting a feel for audience understanding.

*Practical Activities in Cybersecurity*

Weiss et al (2013) suggest that cybersecurity students learn best when they have hands-on experience. The challenge for lecturers and teachers is to ensure that the exercises enable student learning and push students to learn more about cybersecurity. As we shall see later in this chapter when discussing case studies and problem based learning it is difficult in cybersecurity to reflect the complexity of reality and at the same time design activities that can be successful at achieving in relatively short time periods. Practical activities can be stand alone (not linked to other cybersecurity teaching) or more traditionally an opportunity to explore theoretical aspects of cybersecurity from lectures or research in a practical setting. The author has used practical activities in cybersecurity as short sharp learning opportunities, usually linked to a lecture session and as extended learning activities over a longer period of time. Longer activities start to move towards case studies and problem based / project based learning approaches see below.

*Case Studies and Scenarios*

Case studies and scenarios provide examples of people or organisations in real situations which allow learners the opportunity to examine and evaluate authentic problems, as well as apply potential solutions, that will provide clarity as opposed to trying to learn by the study of abstract theories or principles. Case studies attempt to mirror the type of situation that cybersecurity practitioners will encounter in the working environment by providing realistic learning opportunities. One of the interesting opportunities in teaching cybersecurity is the ever growing number of instances that can be used to formulate case studies. It is almost the case that there is at least one significant breach every week that is worthy of study – ranging from attacks against individuals to attacks against organisations and even national states.

In order to address the challenge of realism a case study based approach can be utilised. Use can be made of case studies in both teaching and practical sessions as well in the development of problem solving approach and assessments. This approach provides the opportunity to illustrate the complexity of the cybersecurity environment and allows students to be guided through specific tasks in specific cases whilst at the same time developing their technical skill, their analytical skills and their problem solving abilities.

There is a difficulty in creating case studies both in terms of making them simple enough at one end of the scale to being complex enough at the other. At the same time the case studies need to be authentic and also motivate students. There are ethical considerations, which need to be taken into account when creating cases particularly around the use of live cases (albeit historical live cases) or simulations based on live cases.

The creation of case study material cases for analysis can potentially contravene the rights of those original involved in the cases (even when anonymity is used) issues. Case studies, designed to provide students with appropriate experiences might actually infringe University regulations or even the law – for example when trying to simulate system breaches.

There is a further concern that using case studies based on reality might provide students with ideas for criminal activity that they didn’t have prior to studying the case study. (see discussion on ethics in cybersecurity earlier in the chapter).

*Problem Based Learning*

Problem-based learning (PBL) has been used to positive effect in a number of academic disciplines; Boud and Feletti (1997:1) advocate that PBL is the ‘most significant innovation in education for the professions for many years’. PBL has been used in many disciplines including computer science for a number of years to develop students’ skills in solving authentic and realistic problems. Discussion of PBL examples from the computing science literature include: Nuutila, Törmä, and Malmi (2005), Fee and Holland-Minkley (2010) and van Merriënboer (2013). Kessler (2007:264) discusses the use of PBL in problem solving:

“Ill-defined problems or scenarios can be a fun and interesting way for students to synthesize and/or expand their knowledge, making abstract concepts more real. In PBL problems and scenarios tend to be real, relevant, and tangible, students usually are more motivated to work hard on these projects, often making many real-world assumptions that are applicable to them, further helping to improve their problem solving skills”.

The author was part of a team that developed PBL materials for cybersecurity and one of the objectives of the project was to “improve the efficiency of cybersecurity education and to help students develop the wide range of skills needed to be a cybersecurity professional”. In particular the project attempted to give students the opportunity to develop their cybersecurity understanding by reducing ‘information overload’ and stopping students from learning huge amounts of unnecessary theoretical detail. As part of the application of PBL students had the chance to improve their control over their learning by designing the PBL activities to allow students to self direct, to locate what they need to know and give them possession of their learning.

One of the key aspects identified in the project is that although problem based learning may appear to be the application of common sense (student perception) it is actually a difficult learning skill (set of learning skills) to master. Therefore it is important when using PBL in cybersecurity teaching to include learning guides for tutors and learning guides for learners.

An example of a PBL task in Cybersecurity is given below

In this activity students are encouraged to reflect on the impact of Edward Snowden’s disclosure of National Security Agency documentation. In particular consider the impact on the agencies in the UK, particularly GCHQ, MI5 and MI6.

**Objectives**

The objective of this activity is to analyse the impact of the actions of Edward Snowden in 2013 and the subsequent reaction of the public (impact on society), the security agencies in the UK, USA and around the globe, and an understanding of the legal issues that the scenario raises

**Tasks**

1. Undertake research into the timeline of the main points of the Edward Snowden case
2. Consider the legal, social and ethical issues that should be considered in light of the scenario
3. Identify the implications for the cybersecurity community
4. Relate to other similar scenarios – such as Bradley Manning

**Outputs**

At the end of this activity you should have developed

* your own perspective on the correctness or otherwise of Snowden’s actions

and have created

* a report on the legal issues associated with gathering data on the public;
* a diagram to illustrate the relationship between cybersecurity and surveillance / dataveillance;
* a set of questions from your PBL work on the Snowden example to discuss with your tutor and class.

*MOOCs*

MOOCs are another example of where we can utilise technology in the teaching of cybersecurity. A number of institutions, for example Harvard, provide Massive Open Online Courses (MOOCs) for the public. The Harvard programme (gs.harvardx.harvard.edu/cyber-security/online-course) provides learners with the opportunity to obtain a Harvard certificate. Advocates argue that MOOCs are the future of online education. There has been an exponential growth in the use of MOOCs including in cybersecurity. Although MOOCs don’t normally provide a full coverage of degree they are very useful in prepping students for study of programmes and providing introductions to the cybersecurity subject area. There are two distinct types of MOOC: cMOOC and xMOOC. cMOOCs are collaborative MOOCs that provide learning space for students to collaborate. On the other hand xMOOCs put existing courses into an online format and as such tend to adopt a more traditional format to courses.

*Bootcamps*

Bootcamps appear to be growing in popularity and these tend to be shorter, focussed courses often running for a week or 10 days. Bootcamps offer a different approach to education often being run by industry experts. At the author’s institution we have put in place a series of weeklong bootcamps for final year undergraduate and masters students run by visiting professors. The feedback from students has been very positive about this approach, particularly when it is blended in with a more traditional structure.

*Peer learning*

Students have the opportunity to learn from each other in Higher Education – working in groups, participating in discussion, reviewing demonstrations and undertaking problem based learning are all examples where peer learning can take place in cybersecurity. Boud (1988) suggests that peer learning moves from independent learning to interdependent learning.

There is the potential in peer learning for students to enhance their knowledge of cybersecurity concepts by explaining their understanding to their colleagues and to other students. Peer discussions allow for collaborative working, giving and receiving feedback and potentially evaluating their own learning. Normally peer learning takes place between students in the same class / same level, but at the author’s institution we have also introduced peer support between different levels through a peer mentoring project. The idea was to support learners at lower levels with peers who had been through those levels. Interestingly we found that it was peers at the higher level who benefited most and improved their understanding through the development of their skills in communication, organisation and collaborative support.

**Assessment and Learning in Cybersecurity**

This part of the chapter will examine the ways in which assessment can help learning in cybersecurity and what the assessment might indicate in terms of competence in cybersecurity. There are a variety of assessment instruments which can be used to help learning in cybersecurity including report writing, exams (written, multi-choice, oral), practical tests, portfolios, project work (including research projects, problem based learning projects and work based learning projects) and reflective practice.

Reviewing the literature suggests that assessment is one of the key motivators for students and is fundamental in determining what it is that students value in their education, and this can be applied to cybersecurity education. For example Murphy (2006) suggests that it is assessment that indicates to students what really matters on a module or programme of study and it is assessment that informs students about the goals of the module or programme. As has been indicated earlier the complexity of the cybersecurity environment can provide off-putting for students and assessment tasks may well help with their understanding. There is the potential for assessment to provide a mechanism for student learning and to act as a means of enabling student learning during assessment activities (Rowntree,1987). The concept of “assessment for learning” is proposed as a means to encourage student learning (Black et al, 2003; McDowell et al, 2005).

Brown et al (1997:7-8) put forward the argument that “assessment defines what students regard as important, how they spend their time and how they come to see themselves as individuals”. Gibbs and Simpson (2004) support this perspective summarising that assessment is seen to exert a profound influence on student learning; in areas such as: what students focus their attention on how much they study; the quality of engagement with learning tasks, and, through feedback, on their understanding and future learning. Hamdorf and Hall (2001) indicate that assessment is important because it has such a powerful influence on the learning behaviour of students. Brown el al (1997:7) also identify one of the dilemmas in assessment in that “students take their cues from what is assessed rather than from what lecturers assert is important”. So in designing cybersecurity learning activities we can consider utilising assessment to help students focus on the important aspects.

The principles of assessment (Nicol and Macfarlane-Dick, 2004) require that assessment is reliable, valid, affordable and fit for purpose, i.e. usable. Reliability in assessment requires the assessment to be objective, accurate, repeatable and analytically sound, according to Knight (2001). In essence, reliability refers to the consistency of grades that are awarded and can be affected by marker consistency, inter-marker reliability and / or test / re-test reliability. Validity focuses on the extent to which an assessment measures what it intends to measure and as such contributes to assessing the things programme specifications, programme learning outcomes and module learning outcomes say are important and of value.

The author has employed a number of assessment instruments in cybersecurity to encourage students to use the assessment activities to enable student learning. The use of scenarios to encourage students to think both as attackers and defenders has been particularly helpful in enabling students to understand the cybersecurity environment. As an overall assessment strategy in cybersecurity attempts should be made to:

* get students to identify and critically evaluate threats – ranging from nuisance threats to “advanced persistent threats”;
* design, develop and implement strategies to counter the threats;
* identify when breaches or attacks have taken place and critically evaluate the impact of those;
* design, develop and implement approaches to recover from attack;
* give students the opportunity to evaluate attacks and develop more robust cybersecurity defences as a result.

The above can be done in the context of specific cybersecurity scenarios or case studies, but can also be utilised to encourage students to think about and present policies and procedures for cybersecurity environments.

One particular assessment task that has been used by the author which helps pull together many of the cybersecurity threads and complexities is the use of “infographs”. An extract from an assessment using infographs is given below.

*The cybersecurity environment is a wide and complex one. For the first part of this assignment you are required to produce an infograph (1 page) outlining the typical threats that* ***either*** *a) individuals in society* ***or*** *b) organisations face from breaches of cybersecurity. The design of your infograph and the content of the infograph is left to you to decide but you should consider visual impact, key messages, data to support, examples and underpinning research. You will have the chance to present your infograph to your peers, academics and guests from industry. You should be able to discuss the points raised on your infograph, explaining the detail and answering any questions asked.*

As well as allowing the student to analyse and evaluate a particular issue or concern the assessment enables the development and assessment of a series of professional competencies, including; communication, presentation skills, and the summarising of complex cybersecurity issues.

Theory

Practical

One of the main functions of assessment is to provide a measurement of student understanding – and we can utilise this in cybersecurity teaching to indicate to students where they are in the learning journey, but also to provide an indication to educators as to how well the students have grasped the cybersecurity concepts, [note – this can be an important aspect if assessment is to be used for certification, see discussion earlier in the chapter]. There is an argument put forward in Black (1999:118) who suggests summative assessment “serves to inform an overall judgement of achievement, which may be needed for reporting and review”. Pelligrino et al (2001:42) support this position proposing that “assessment is a tool designed to observe students’ behaviour and produce data that can be used to draw reasonable inferences about what students know”.

However, there has also been a level of concern regarding the appropriateness of this use of assessment for example, Biggs (1996) suggests that “testing has not always promoted good learning and indeed can have detrimental effects” and Black and Wiliam (1998), argue that summative assessment is not a particularly good means of finding out what it is that students know.

When students participate in assessment – both summative and formative – it provides an opportunity to give feedback to students. The provision of feedback is one of the primary functions of assessment and can enhance student learning. One of the key ways that we can use assessment to help with learning is through constructive feedback on assessment activities. When we design cybersecurity assessment activities and when we generate feedback we need to make sure that students value the process and have time to engage in the process. Nicol and Macfarlane-Dick (2004:3) suggest that formative assessment and feedback should be “used to empower students as self-regulated learners and that more recognitions should be given to the role of feedback on learners’ motivational beliefs and self-esteem”. If we use the rationale of empowerment and encourage students in the direction of wanting to learn then the value of assessment activities and the value of participating in those activities should become apparent.

Teachers in higher education put a great deal of time and effort into producing written, and indeed, oral feedback. We have already seen that there is a huge amount of assessment and a growing number of students. Despite the changing environment of mass education students want the feedback process to be clear, explicit and fair (Holmes and Smith, 2003). If feedback is to contribute to student learning in cybersecurity and we put a great deal of effort into it – how can we be sure that it is having the desired effect on helping students?

Perhaps the simplest reason that students want feedback is that it will help them to learn. However, it is not quite as simple as that. The situation is also further complicated in that the types of feedback which are most effective will vary depending on the cybersecurity task being assessed. We need to make sure that the feedback that we provide will actually be useful and usable for students, by this we mean that feedback should:

* be understandable by students – there is the possibility that the feedback provided to students is often not understood by the students.
* be valued by students – in order to be valued by students feedback should be constructive and reflect the effort that they have put into any assessment activities but also be meaningful in the context of their future learning needs (feed-forward).
* allow students to “close the gap” on their understanding – if students know what to do to improve they can “close the gap” between what they can do or know and what they need to do or know then there is the potential to make that learning opportunity effective.
* be of appropriate quality – the quality of feedback given to learners has a significant impact on the quality of learning. The feedback should provide information that helps students trouble-shoot their own assessment performance and take action to close the gap between intent and effect.
* be timely – one of the key aspects in enhancing efficiency of learning is to ensure that feedback on assessment is timely. If students don’t get the feedback soon enough then feedback is less likely to be perceived to be useful for their on-going studies.

Assessment tasks and the feedback associated with the assessment tasks provide an efficient and effective set of instruments to help students enhance their cybersecurity learning. It is important to think about the assessment design, the expectation of the assessment task and the resultant feedback (as well as the ways in which the student will be able to use the feedback).

## Inclusiveness and Diversity

In mass education systems, such as today’s Higher Education provision, we need to remember that not all students are the same, the learning needs for students will vary and there will be a wide range of student learning experiences.

As with all educational activities there is a need to consider the nature of cybersecurity learning activities for diverse student groups taking into account legislation such as the Disability Discrimination Act (1995) and the Special Education Needs and Discrimination Act (SENDA) (2014).

## Cybersecurity activities provide us with an opportunity to address inclusiveness and diversity. There has been a large amount of work on diversity undertaken by the HE Academy (for example, HEFCE, 2002; HE Academy, 2006) and from organisations such as the National Disability Team (see http://www.techdis.ac.uk). However, the vast majority of this work focuses on teaching practice rather than on specifics about teaching cybersecurity.

A great deal of the work on diversity has been reactive in nature – i.e. we are aware of a student or group of students with particular needs and we put in place mechanisms to allow the students to participate equally in the cybersecurity learning activities. However, if we are more proactive and consider inclusiveness for all students when we are designing our cybersecurity activities then the reliance on a reactive approach should diminish. The process of addressing diversity in cybersecurity and attempting to make learning and teaching on cybersecurity inclusive can be of benefit to all students as we consider in detail the expectations we place on the activities, the impact of the activities on the students and the potential problems that may arise from the learning and teaching.

It is suggested that equality and diversity issues can be proactively addressed by addressing the inclusiveness in cybersecurity activities. Addressing inclusiveness will be a benefit for all students because if the improved levels of consideration are given to the cybersecurity learning design the activity will be enhanced for all.

**Summary and Conclusions**

This chapter has drawn on current research and best practice on teaching and assessment in cybersecurity in higher education. We have considered the theoretical and pedagogical foundations for helping tutors make decisions about the methods and approaches to utilize in teaching and assessing the cybersecurity curriculum.

As has been discussed in this chapter there are many variables to take into account when considering effective teaching in cybersecurity. Irrespective of the variables or the objectives in the teaching it is important to focus on the learning needs of the participating student. The needs of the student will vary depending on the level of learning and the prior subject knowledge of the learner. The emphasis in this chapter has been to encourage providers to design cybersecurity teaching and learning opportunities that provide systematic and stimulating learning experiences that will give students the best chance to succeed in their learning. We have advocated that providers ensure that:

* learning is transparent;
* teaching activities facilitate dialogue between teachers and learners and between learners; and
* we develop communities of learners.

The principles and theories of cybersecurity and the associated application of those principles and theories exist in an ever-changing and rapidly developing environment. The environment is complex and complicated which provides further challenges for those seeking to teach cybersecurity effectively.

**References**

ACM (2017) *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. A Report in the Computing Curricula Series Joint Task Force on Cybersecurity Education*, available at <https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf> accessed June 2018

Alvarez, B. (2011) ‘Flipping the classroom: Homework in class, lessons at home’ in *Education Digest: Essential Readings Condensed For Quick Review*, Vol. 77 No. 8 pp 18 – 21

Biggs, J., (1996) ‘Assessment learning quality: reconciling institutional, staff and educational demands, in *Assessment and Evaluation in Higher Education*, Vol 12, no 1, pp 5 – 15

Black, P., (1993) ‘Formative and summative assessment by teachers’, in *Studies in Science Education*, Vol 21. pp 49 – 97

Black, P. and Wiliam, D, (1998) ‘Assessment and classroom learning’, *Assessment in Education* Vol. 5 No. 1 pp 7 - 74

Black, P. and Wiliam, D., (1999) *Assessment for Learning: Beyond the Black Box. Cambridge*, Assessment Reform Group, University of Cambridge, pamphlet 371.26 ASS, available at <http://www.assessment-reform-group.org.uk/AssessInsides.pdf> accessed June 2018

Boud, D., Cohen, R., and Sampson, J., (1988) ‘Peer Learning and Assessment’ in *Assessment and Evaluation in Higher Education*, Vol 24, No 4, pp 413 - 426

Boud, D., & Feletti, G. (1997). *The challenges of problem based learning*. London: Kogan Page

Brown, G., Bull, J., and Pendelbury, M., (1997) *Assessing Student Learning in Higher Education*, London, Routledge

Cohen, P. A. (1981) ‘Student ratings of institution and student achievement: a meta-analysis of multisection validity studies’, in *Review of Educational Research*, Vol. 51, pp 281 - 309

Covill, A., (2011) ‘College students’ perceptions of the traditional lecture method’, in *College Student Journal*, Vol 45, Issue 1, pp 92 - 101

Disability Discrimination Act (1995) with Amendments (2000) available at http://www.legislation.hmso.gov.uk/acts/acts1995/Ukpga\_19950050\_en\_1.htm (accessed July 2018)

Fee, S.B., & Holland-Minkley, A.M. (2010). Teaching computer science through problems, not solutions. *Computer Science Education, 20*, 129–144

Garet, M.S., Porter, A. C., Desimone, L., Birman, B. F., Yoon, K. S., (2001) ‘What Makes Professional Development Effective? Results from a National Sample of Teachers’ in *American Educational Research Journal*, Vol. 38, No. 4 pp 915 – 945

Gibbs, G., and Simpson, C., (2004) ‘Conditions under which assessment supports students’ learning’, in *Learning and Teaching in Higher Education*, Vol. 1, No. 1, pp 3 – 31

Hamdorf, J. and Hall, J.C. (2001) ‘The development of undergraduate curricula in surgery assessment’, in The Australian & New Zealand Journal of Surgery, Vol 71, pp 178-183

Harris, M. A., and Patten, K., (2015) ‘Using Bloom’s and Web’s Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum’, in Journal of Information Systems Education, Vol. 26, No., 3, pp 219 – 229

HEFCE 2002/48 Successful Student Diversity, available at http://www.hefce.ac.uk/pubs/hefce/2002/02\_48.htm (accessed July 2018)

Higher Education Academy (2006) Embedding Success Enhancing the Learning Experience for Disabled Students, York, Higher Education Academy

Holmes, L., and Smith, L., (2003) ‘Student evaluation of faculty grading methods’, *Journal of Education for Business*, July / August 2003, pp 318 - 323

Irons, A. D. and Devlin, S., (2012) ‘The Inspiring Teacher in Computing’, paper presented at *1stAnnual Conference on Aiming for Excellence in STEM Learning and Teaching*, Imperial, London, 12th-13th April 2012

Irons, A. D., Savage, N., Maple, C., and Davies, A., (2016) ‘Embedding Cybersecurity in the Computer Science Curriculum’, in *IT Now*, Summer 2016, pp 56 – 57

Irons, A. D., and Thomas, p., (2016) ‘Problem based learning in digital forensics’, in *Higher Education Pedagogies*, vol 1 No 1, pp 95 – 105

Jenkins, A., and Healy, M., (2005) *Institutional strategies to link teaching  
and research* Higher Education Academy Publication, available at <https://www.lir.gu.se/digitalAssets/1345/1345048_institutional_strategies.pdf>, accessed June 2018

Johnston, N., and Karafotias, T. (2016) ‘Flipping the Classroom to Meet the Diverse Learning Needs of Library and Information Studies (LIS) Students’, in *Journal of Education For Library and Information Science*, Vol 57 No 3, pp 226 – 238

Joshi, P., Thukral, A., Joshi, M., Deorari, A. K., Vatsa, M., (2011) ‘Comparing the Effectiveness of Webinars and Participatory Learning on Essential Newborn Care (ENBC) in the Class Room in Terms of Acquisition of Knowledge and Skills of Student Nurses: A Randomized Controlled Trial’ in Indina J Pediatr, available at https://www.researchgate.net/profile/Anu\_Thukral/publication/224914755 accessed June 2018

Kessler, G.C. (2007). Online education in computer and digital forensics: A case study. In *IEEE* *Proceedings of the 40th Hawaii International Conference on System Sciences 2007*. Honolulu

Knight, P., (2001) *Formative and Summative, Criterion and Norm-Referenced Assessment*, LTSN Generic Centre, Assessment Series No. 7

Lundstedt, S., (1966) ‘Criteria for Effective Teaching’, in Improving College and University Teaching, vol 14 no 1, pp 27-31, available at <https://www.tandfonline.com/doi/abs/10.1080/00193089.1966.10532492?src=recsys>, accessed June 2018

McDowell, L., Sambell, K., Bazin, V., Penlington, R., Wakelin, D. Wickes, H. and Smailes, J. (2005) ‘Assessment for Learning: Current Practice Exemplars from the Centre for Excellence in Teaching and Learning’, *Northumbria University Red Guides,* Series 11, Paper 17

McGettreick, A., (2013) ‘Toward effective cybersecurity education’, in *IEEE Security and Privacy*, Voll 11, Issue 6, 66 – 68

Murphy, R., (2006) ‘Evaluating new priorities for assessment in higher education’, in Bryan C., and Clegg, K., (eds) (2006), *Innovative Assessment in Higher Education*, London, Routledege, pp 37 – 47

NCSC (2018) ‘New Cyber Attack categorisation system to improve UK response to incidents’, available at <https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents>, accessed June 2018

Nicol, D., and Macfarlane-Dick, D., (2004) ‘Rethinking formative assessment in HE’ in Juwah, C., Mcfalane-Dick, D., Matthew, B., Nicol, D., Ross, D, and Smith, B., (2004) *Enhancing Student Learning Through Effective Formative Feedback*, HE Academy, pp 3 – 14

Nuutila, E., Törmä, S., & Malmi, L. (2005). PBL and computer programming — The seven steps method with adaptations. *Computer Science Education, 15*, 123–142

Oltsik, J., (2017) The Life and Times of Cybersecurity Professionals, ESG, ISSA Report, available at <https://www.esg-global.com/hubfs/issa/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Nov-2017.pdf> accessed June 2018

Pelligrino, J. W., Chudowsky, N., and Glaser, R., (editors) *Knowing what Students Know – The Science and Design of Educational Assessment*, National Academic Press, Washington D.C

Rowntree, D., (1987) *Assessing Students: How Shall we Know Them ?* 2nd edition, London, Kogan Page

Weiss, R., Mache, J., and Nilsen, E., (2013) ‘Top 10 hands-on cybersecurity exercises’, in *Journal of Computing Sciences in Colleges*, Vol 29, Issue 1, pp 140 – 147

Williams, J., and Cappuccini‐Ansfield, G., (2007) ‘Fitness for Purpose? National and Institutional Approaches to Publicising the Student Voice’, in *Quality in Higher Education*, Vol. 13, No 2, pp 159-172

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., and Sommer, P. M. (2003) ‘Computer Forensics Education’, *IEEE Security & Privacy*, Jul-Aug 2003, Volume 1, Issue: 4, pp. 15-23