Chapter 1
Designing and Developing a Scenario Based Curriculum for Cyber Education in HE

Rosanne English

Abstract Designing cyber security courses in Higher Education can be a balancing act between an understanding of the theory of cyber security and the practicality of application of this knowledge to a changing landscape. Scenario-based learning is an active learning technique which offers a potential bridge between these two goals, allowing learners to both achieve an understanding of core concepts whilst being asked to apply them to more complex and imprecise problems [2]. This chapter presents a case study which documents the application of scenario-based learning to a cyber security module, highlighting the rationale behind using this technique, how the module was designed with scenario-based learning at its core, and guidance for the reader who may wish to apply this technique to their own security modules.

1.1 Introduction

Cyber security is a key component of computing science degrees. Indeed many non-computing degrees now also incorporate cyber security as its prominence becomes increasingly more relevant and in demand [22]. For example, within the UK Northumbria University offers a Cybersecurity Law Masters programme [23], the University of Glasgow offers a [24] and the University of Portsmouth offers a Cybercrime Masters programme [25]. Each of these programmes are not offered by computing departments, though some do have modules within the programmes delivered by computing science departments.

University offerings such as those mentioned provide an opportunity to bridge the cyber security skills gap which has been estimated at 3.5 million unfilled cyber security jobs by 2025 [22]. More traditional offerings within generalised computing degrees are also increasing cyber security provision, particularly where accreditation requires it. For example, in the U.K. the British Computer Society increased

Rosanne English
University of Strathclyde, Glasgow, Scotland e-mail: Rosanne.English@strath.ac.uk

their cyber security requirements in 2015 [13] However, delivery of cyber security in an academic environment also introduces a number of challenges.

One challenge is how such a module or programme should be taught. As noted by Schneider, some perceive the approach should be to teach the adversarial mindset through exploration of specific attacks, whilst others believe it should focus on the principals and concepts [3]. In the first approach, some students are able to generalise and develop the mindset such that they are then able to apply it to new contexts. However, others are less able to do so. As Schneider notes, those students who are by themselves unable to create an abstract mental model are disadvantaged since they are unable to move with the fast-paced changes in cyber security. In contrast, using a more principal focused approach can result in students developing only a theoretical understanding and potential dissatisfaction due to lack of perceived 'practicality'.

In order to better support students in understanding a combination of principles and practice to develop conceptual understanding as well as the adversarial mindset, a different approach to design might be helpful. This chapter will present a scenario-based approach to designing a cyber security module, which aims to help students understand principles as well as providing practice in applying these to different contexts.

1.2 How to Use this Chapter

It is anticipated that readers may approach this chapter with different goals in mind. In general you could fall into one of three categories;

1. You wish to gain an appreciation of scenario-based learning and how it may be applied to a security module design
2. You wish to develop a complete module which uses scenario-based learning as the key teaching technique
3. You wish to apply scenario-based learning to part of a module such as a single topic

Should you fall into the first category, it is suggested you approach this chapter by reading Section 1.3, which provides the background of scenario-based learning and presents the philosophy of why this could be helpful in a security module. You can then explore Section 1.4 which presents the design process and finish with the conclusion for a reflection on the delivery of this approach.

Should you fall into the second category, it is suggested that you may skip Section 1.3 on the philosophy of this approach and the background and instead focus on Section 1.4 which introduces the design process of this case study. The hope is that having read the design approach, one can consider how this may be applied in one's own context. Having done so, you can then consider the reflection on delivery of the module which is presented in Section 1.5. Section 1.5 is split into three aspects; structure, facilitating sessions, and assessment. Structure and facilitation aim to provide insight into the practicalities of delivery of such a module, whilst assessment

provides a reflection on the types of assessment one may consider. As such, if one has their own assessment already in mind, this aspect can be missed.

Should you fall into the third category, you may wish to consider Section 1.3 if you are trying to determine why one might wish to use SBL. You could then read Section 1.4 which addresses the design, though if applying to a single topic you should bear this in mind as the case study discusses a module as a whole. In Section 1.5 on delivery, you may wish to focus more on the Facilitating Sessions element as this is applicable to a smaller set, whilst overall structure and assessment may be less helpful.

1.3 Bridging the Gap Between Theory and Application: Considering Learning Models for Cyber Security

In determining how to bridge the gap between theory and practice approaches to teaching cyber security, we can look to constructive learning design which focuses on students actively constructing their knowledge and understanding through authentic tasks which have clear objectives [28]. Constructivism is well established within computing science education [17] and its guiding principle is that students learn through experience, and connect learning to prior experiences to build mental schemas [16]. Using a constructivist technique applied to cyber security provides an appropriate learning model lens to design a module on.

Advocates of constructivism emphasise seven key goals for constructivist learning [14]. Each goal is considered below, with a reflection on how they align with the objective of teaching cyber security in a way which bridges principles and practice.

1. **Experience should be combined with knowledge construction** This goal aligns with the aim of combining the two general approaches to teaching cyber security as proposed by Schneider [3].
2. **Experience and appreciation of multiple viewpoints** This goal emphasises how there are often multiple acceptable solutions or perspectives for any given problem within a context. Honebein argues that it is important for learners to be able to consider a range of alternative solutions and engage in evaluating and testing the most appropriate solution instead of fixating on one correct solution [14]. This is especially important in cyber security, e.g. in encryption there are multiple ciphers and the best solution can depend on the context.
3. **Embed learning in realistic contexts**: This goal supports the need to ensure the learning context is relevant and realistic. In 1991 Lave and Wegner [1] introduced the concept of situational learning, which describes this goal. Situational learning can be thought of as learning which happens within the appropriate context. Lave and Wegner argue that situational learning is essential for acquisition of professional skills and that one cannot and should not remove the context from the learning process. The reasoning is that without context, concepts are taught in isolation and this limits a learner's ability to adapt to different contexts. This is of

particular importance in cyber security where it is critical that learners are able to apply understanding of core concepts, such as encryption and network security, to new situations and thus bridge the gap between theory and application. Learning concepts entirely independent of context is sub-optimal as it would introduce a challenge for a learner to transition to applying these in the real world.

4. **Promote student ownership of learning**: this aims to ensure students engage and take responsibility for their learning over passive consumption of knowledge sometimes referred to as shallow learning. To be able to combine principles and practice this is important aim. Biggs [26] argues that more active learning activities encourages deep learning.
5. **Immerse learning in a social space**: this emphasises the benefit of learning within a social space, e.g. through group discussions.
6. **Encode learning in multiple formats**: This relates to a variety of formats for learning materials to support learners in being able to learn from various sources.
7. **Develop student metacognition and reflexive practice**: Metacognition can be thought of as an individual's understanding and regulation of their learning. Developing metacognition is a key factor in helping learners develop the skills to work in a rapidly changing environment such as cyber security. Consequently, it is important to chose a learning model with this in mind to ensure learners are well scaffolded to understand cyber security. Volet [15] conducted experiments which showed that metacognition and learning outcomes were improved both in the short and long term where content-relevant metacognition strategies were modelled and a socially supportive learning environment was employed. As a result, a learning model which allows adaption to the context of cyber security is important.

Having now established constructivism as an appropriate guiding principle, we can now consider how this model can be implemented through active learning techniques. In order to ensure realistic contexts and immersion in social spaces, In 1991 Lave and Wegner [1] introduced the concept of situational learning, which can be thought of as learning which happens within the appropriate context. They argue that situational learning is essential for acquisition of professional skills and that one cannot and should not remove the context from the learning process. The reasoning is that without context, concepts are taught in isolation and this limits a learner's ability to adapt to different contexts.

1.3.1 Problem Based Learning

One pedagogical model which aligns with constructivist and situational learning is problem-based learning (PBL). In a problem based learning design, students are placed into small groups and are given a problem which they must explore and present a solution for. A tutor is provided for each group to act as a guide, ensuring students stay on task and assisting where necessary.

Problem-based learning has been considered in regards to cyber security for similar reasons to those outlined in this chapter. For example, the work by Shivapurkar [12] and the Cyber Security Knowledge Exchange project [27].

Shivapurkar *et al.* use the structure of Maastricht University on problem-based learning [12] to demonstrate how this could be applied to cyber security education. In their paper the authors present two scenarios. The first scenario asks students to consider how they could execute phishing attacks, requiring students to identify what phishing attacks are and the practicalities of trying to implement such an attack. The second problem focuses on an attack on a Windows SMB port which allows the attacker to steal a file, and asks students to determine how such an attack could be executed as well as which techniques they could use to stop such an attack. However, the paper indicates that applying this within a course had not yet taken place.

Unfortunately the AdvanceHE project website appears to be no longer maintained, thus it was not possible to access the resources or develop an understanding of how it was achieved. However, reviewing the presentation from the AdvanceHE website shows that the motivation behind the project was similar, in that the intention was to help students develop the skills of evaluating a system on the basis of its security.

The PBL model is typically used as the primary mode of teaching throughout a given module, and tends to make use of larger more complex problems with multiple sources of information for learners. Learners in PBL also need to set their own learning objectives and identify areas they need to learn before being able to tackle the problem [9].

Barrows [18] identified six characteristics of PBL as follows:

1. Learner centred
2. Small student groups supported by tutor
3. Tutor acts as a facilitator
4. Problems should be authentic
5. Problems should be designed such that learners must develop the required knowledge and skills to solve them
6. New knowledge should be acquired through self-directed learning

As class sizes grow, it is unlikely that resources would be available to ensure that characteristics 2 and 3 are met. Similarly, it can be difficult to structure self-directed learning with increasingly diverse cohorts. Developing more complex problems with multiple information sources can also be challenging for a single educator to implement for a complete course.

This can be seen in the work by Moust *et al.* who reviewed the practical implementation of the Maastricht University PBL approach [19]. The authors note a demise in the seven step process for implementing PBL which was established along with the University approximately 30 years prior. For example, they observed students were less likely to perform self-directed learning and literature searches, and student-staff ratios were not sufficiently adequate as to allow this approach. Consequently an alternative approach was considered.

1.3.2 Scenario Based Learning

Scenario-based learning was identified as a constructivist approach similar to problem-based learning which still helps bridge the gap between theory and practice whilst providing more scalability to combat the challenges of implementing PBL.

A scenario-based approach provides students with problem scenarios which they have to explore and present solutions to.

Scenario Based Learning often focuses on written scenarios as the primary source and is not the only method used within teaching. It is also more flexible which means it can be adapted for larger class sizes with less resource, whilst also ensuring students get sufficient scaffolding to support a diverse cohort of learners.

Similarities between SBL and PBL include the need for a realistic scenario, which has elements which are not clearly defined to mimic the uncertainty of the real world [9] .

Scenario based learning is a technique which aligns with situational learning by provision of context through scenarios. It provides learners a real world style context in which they apply their knowledge and skills. The technique can help students engage with the material due to the connection with an authentic context [5].

Scenario Based Learning can have a number of positive effects on the student learning journey. It can improve student motivation, critical thinking, and problem-solving (Norton et al., 2012). Such an approach helps shift learners from a knowledge-based exploration of cyber security to higher cognitive skills [11]. As a result, scenario based learning suits itself well to cyber security as a field.

Whilst there is little on how to approach the design and development of a cyber module which uses the scenario or problem based approach, there is some literature around designing such modules for other subjects. Notably, Wolfe presents the design of a database security module with a single scenario as the focus for exploring database security [10]. In particular the following elements are identified:

- Place the student into the narrative
- Base the scenario on a real situation
- Use small businesses rather than large
- Incorporate realistic defects
- Simplify business circumstances

Firstly, placing the student into the narrative of the scenario gives the student a role to play in the situation [10]. Aspects for consideration in this role are the objective of the role, what they can and cannot do (e.g. levels of authority). Another key element is authenticity. Wolfe describes this as ‘realism’ of the scenario. This could be achieved in a number of ways, such as simplification of a larger problem seen in the real world either experienced personally, experienced by colleagues or friends, and examples from the news.

The size of the scenario, whilst trying to be realistic, is necessarily limited in complexity. This is due to the time and resource available for a given module or teaching session. One element to consider here is the size of the business used in a scenario. As argued by Wolfe [10], the complexity of larger organsiations would

pose too much of a challenge for students to meaningfully explore in the limited time frame of a module. This is particularly important if a scenario is only used for exploration of one topic. As a result, smaller businesses or more contained scenarios allow a sufficiently authentic problem without overwhelming students.

Also related to authenticity is the need to incorporate realistic defects. The aim of a security module is to help learners understand the kinds of security vulnerabilities and identify corresponding mitigation techniques. By modelling realistic defects, this provides learners the opportunity to assess a given context in terms of security. However, once more one needs to be careful that there are not so many issues such that it might overwhelm the learners.

Summarising these attributes for developing security scenarios, the following criteria for developing security scenarios are proposed:

- Authenticity with limitations
- Incorporate realistic defects
- Simplify business circumstances

Having decided on an appropriate technique and identified criteria for developing cyber security scenarios, the next step is to explore how this can be applied to the design of a cyber security module. This is addressed in the next section which presents a case study covering the design of a cyber security model.

1.4 Designing a Scenario-based Cyber Security Module

This section outlines the approach taken in designing the curriculum of a scenario-based cyber security module. The module is a UK based final honours year cyber security fundamentals module. It starts by considering the intended learning objectives (ILOs) and corresponding content, then the development of scenarios followed by the delivery structure.

The proposed procedure for development of scenarios is a 6 step process as follows:

1. Identify module ILOs related to this task
2. Identify related tasks necessary to achieve ILO(s) from step 1
3. Identify appropriate contexts, e.g. small medical practice
4. Write the scenario incorporating the tasks and context from steps 2 and 3
5. Ensure the scenario is appropriate and revise as necessary
6. Develop assessment

These steps will be covered in detail in the remainder of this section.

1.4.1 Learning Outcomes and Identifying Tasks

In identifying a suitable structure and content for the module, it is recommended to use a constructive alignment approach. As noted by Biggs [26], this approach requires the setting of intended learning outcomes prior to teaching and designing learning activities which give learners the opportunity to engage with that task. In this application, the scenario-based questions are the primary learning activities.

In developing the intended learning outcomes for a module it can be helpful to use the cognitive domain Bloom's taxonomy ([21]) or the revised taxonomy ([20]) to ensure the objectives are set at an appropriate level. Bloom's taxonomy allows the level appropriate verbs to include in the intended learning outcomes. For example, evaluation would typically be expected in hours years as well as in Masters programmes. Thus if exploring a range of cryptography protocols, evaluation of an appropriate protocol to apply in a given situation would be more suitable at higher levels than exploring the knowledge levels like explain the TLS protocol. However, it should be noted that in order to demonstrate higher levels of achievement, it is necessary to work through the lower levels related to knowledge and understanding.

The following learning outcomes are those for a foundational cyber security module which covers core concepts of cryptography and secure communication, network security, and user authentication and access control. Additionally, the skill of analysing threats and evaluating secure solutions is important to develop a security mindset.

- Differentiate between secure communication information security solutions to determine an appropriate solution for a given context
- Evaluate an existing or proposed system in terms of potential security vulnerabilities and recommend the most appropriate security solution to apply
- Critique the security of a given network scenario and propose appropriate mitigation techniques
- Perform to analysis of cyber risk and threat modelling

Having now identified learning outcomes, the next step is to identify the content which allows those objectives to be achieved. This constructive alignment approach throughout the design process ensures students are scaffolded in being able to achieve these objectives.

The following is a proposed structure for an introductory cyber security module which aligns with the ILOs above and prioritises the key concepts of cryptography, authentication and access control, and network security as the core areas which allow exploration of other fields such as web security and human aspects of security.

It is now possible to break down each topic into further content elements. For example, which specific cryptographic protocols are to be covered etc. Having such a breakdown then permits the lecturer to decide an appropriate range of material to support students in achieving the ILOs.

The content can then be the basis of developed comprehension materials such as lectures, videos, reading etc. Note that a mix of media can be helpful to keep learners engaged.

Week	Topic	Sample subtopics
1	Principles of Cyber Security	CIA triad, important terminology, related legislation
2	Cryptography	Cryptography primitives such as cryptographic hashes, components and overview of encryption
3	Cryptography	Further cryptography e.g. PK Infrastructure and Digital Signatures
4	Authentication and Access Control	Authentication factors, access control models, biometric authentication, secure password management
5	Network Security Attacks	Attacks such as Machine in the Middle, replay attacks and Denial of Service
6	Network Security Defence	Defence mechanisms e.g. firewalls, Demilitarised Zones, VPNs and TLS
7	Malware	structure and mitigation
8	Web security	OWASP Top 10 and mitigation techniques
9	Cyber Risk Management	Stages of risk management
10	Human-Centred Security	Phishing, Social engineering

Table 1.1 Overview of Topics

Having now determined the appropriate ILOs and corresponding content, the next step is to develop scenarios which allow learners the chance to practice skills which demonstrate the ILOs.

1.4.2 Identifying Context and Developing Scenarios

Having determined the ILOs and topics, one can then consider the components a student must understand in order to be able to engage fully with a scenario.

For example, let us consider the following learning objective- ”differentiate between secure communication information security solutions to determine an appropriate solution for a given context”. This objective can be further broken into the following tasks:

- understanding of components of modern ciphers and how they are used in different ciphers
- compare and contrast different ciphers for different purposes
- evaluate a scenario to determine the most appropriate cryptographic solution

A related scenario then must ensure an opportunity to demonstrate understanding of cryptography primitives and their use in ciphers, compare different ciphers, and justify a choice been different ciphers for the given scenario.

Having identified the ILOs and related task breakdown, the next step is to identify an appropriate context. The following are some examples of contexts:

- a small software development business (helpful when looking at technical elements)
- a medical practice (helpful when exploring access to particularly sensitive data)

- a friend seeking advice e.g. on aspects of cryptography to ensure security of their data (helpful in ensuring comprehension)

Of course, there are many more possible contexts. It can be helpful to keep up to date with recent cyber attacks which can provide inspiration for the context. For example, the Wannacry ransomware attack could be abstracted into an example of software not being updated and malware exploiting a vulnerability in non-patched software. Students could be asked to consider the mitigation techniques which may have prevented this, in particular more substantial procedures may have mitigated the issue of some branches not updating software with a known vulnerability. This is a helpful example to highlight that technical controls are not the only option, an element which can be overlooked by students with a penchant for technical solutions.

We will continue with the example cryptography example where we identified tasks as; demonstrate understanding of cryptography primitives and their use in ciphers, compare different ciphers, and justify a choice been different ciphers for the given scenario. The context we will use will be a friend seeking advice.

Having now selected a context, the scenario can be written to incorporate the tasks with the context. A scenario could then be:

A friend is building a dynamic website for their local sports club of which they are a board member. Information on members of the club must be stored securely in a database. Your friend is confident in developing the code and interface, but is unsure of the best choices in regards to data security. In particular, they wish to use a block cipher but do not know how to differentiate between a block cipher and a stream cipher. As your friend is aware of your experience in cyber security they have asked for your help.

1. Your friend asks you to explain the difference between block and stream ciphers, and why you may chose one over another
2. Having clarified this, your friend is now aware of two block ciphers - AES and Blowfish. They wish to understand the distinction in the mechanisms used within these ciphers, and whether they should chose one over the other for storing sensitive data which is not passwords. Provide a comparison of the ciphers along with an evaluation as to whether one cipher would be more suitable for this context over the other.

Recall it is helpful to place the learner into the narrative, in this instance the learner is being asked for help. We can also ensure all elements of the tasks have been covered, the task is realistic (indeed the author was asked to complete a similar task) and circumstances have been simplified as there is no mention of GDPR or consideration of how the data is gathered, as well as consideration of physical security storage.

Other examples can include those such as the Wannacry example, which is authentic with a realistic defect and business circumstances can be simplified by lack of consideration of the connection and different approaches between different areas or branches. In terms of incorporating the student into such a scenario, they could be employed as a security consultant to explore what led to the incident and how to mitigate against a similar issue in the future.

To ensure consistency and clarity, a proposed proforma which provides the structure of a scenario-based activity is provided in Table 1.2.

Element	**Description**
Module ILOs:	The ILOs for the module as they relate to this scenario-based activity
Key skills:	The breakdown of skills which allow the above ILO(s) to be demonstrated
Scenario Context:	The narrative of the scenario.
Questions	Specific prompts and questions for learners to answer

Table 1.2 A proforma structure for a scenario-based activity design

1.4.3 Assessment

The assessment should allow students to apply skills developed through completion of the SBL exercises. For example, one form of assessment would be a scenario-based written exam. This is an exam where the questions are structured in the same format as the scenario-based questions throughout the module. However, it should be more constrained than those used in facilitated sessions as questions and scenarios which are too open can overwhelm students within an exam setting. An overly open question can also mean learners struggle to interpret what is being asked, and consequently answers may be more varied than is optimal.

If using an exam, it is worth considering making it an open book exam where students can reference their notes. The reasoning is that it reduces the need for students to perform rote memorisation and instead focuses on the comprehension of concepts and being able to perform the skills required by the ILOs. However, this can introduce issues with academic integrity, as such it is worth reminding learners of expected standards.

A sample exam question context is provided as follows. You have a friend who has set up their small business computer network and are working to secure it. They do not understand much about network security and have asked for your help. On their network they have a file server which they wish to be able to access from outside their business network.

A corresponding question could then be ”Propose and justify a firewall structure which would allow your friend to access their server from the internet but would not expose the local address of the server.”

It is also possible to make use of coursework which makes use of the scenarios. For example, a case study analysis could be an appropriate coursework. In such an

assessment, learners would be asked to identify (or pick from a select list) a recent security incident and analyse what went wrong, and what mitigation strategies might be suitable for the given context. This also has the benefit of providing learners with an opportunity to refine their communication skills.

Coursework can also use a scenario which provides the context for the assignment. For example, learners are asked to imagine they are part of a red or blue team and they have been tasked with assessing the security of a given system and then to report their findings. This approach has the benefit of a balance between hands on activities and reflective evaluation.

There are likely many more options which accommodate this style, but hopefully the few examples above provide inspiration as to what might be possible.

We have now addressed how one can approach designing scenario-based activities. The next element to consider is how these activities combine into a delivery approach for the module as a whole. This is addressed in the next section where a series of steps to designing a scenario-based cyber module are provided with a breakdown of each step.

1.5 Delivery

At this stage, one should now have a clear overview of the module ILOs, the content, and the scenarios and corresponding tasks as well as assessment. The next step is to put this together into a structure for delivery. This section aims to address this, providing insight into some of the challenges and logistics of delivery. This is split into three areas; structure, facilitating SBL sessions, and assessment.

1.5.1 Structure

By incorporating scenario-based learning one might anticipate the required contact hours would increase. If traditional content delivery (e.g. through didactic lectures) is maintained then this would be the case, as the lecturer should be on hand to facilitate learner explorations of scenarios. However, a more appropriate approach would be to use the flipped classroom model for delivery. This is one way to ensure the content is delivered to students whilst making space for the content checking and scenario engagement essential for scenario based learning to take place.

Baker [7] coins the term flipping the classroom as an instructional model where the content element (the traditional lecture) is removed from the in class time. Learners are expected to engage with the content prior to attending class. The reasoning being that meaningful application of concepts and techniques can then take place with the instructor on hand to be the ”guide on the side” [8]. The content of the module can take the format of pre-recorded lecture videos, or reading or other ac-

tivities. The key element is that students must engage with the material prior to the sessions with the lecturer to ensure they get the most of the interactive elements.

The structure of a typical week is then as shown in Fig 1.1. From Fig 1.1 one can see that the lecturer should ensure material which requires students to engage with it prior to a facilitated session should be made available sufficiently far in advance. Giving learners as much time as you can to process the content is ideal, as is setting a consistent day to release such content. One approach could be that material for a given week is release on the Monday in the week prior. This provides students with at least one week to engage with the content.

You may also wish to have activities which students can complete in order to concept check. This helps students identify misunderstandings prior to engaging with the scenarios. There are a range of options including activities such as multiple choice (which has the benefit of automated marking and feedback) or minute papers, or if class time permits then a more traditional tutorial which checks fundamental comprehension and application of module content material. It is helpful for the lecturer to be able to identify any common areas of confusion and directly address these either asynchronously through the Virtual Learning Environment (or other communication channel) or whilst in a class session which allows for a conversation with learners to take place.

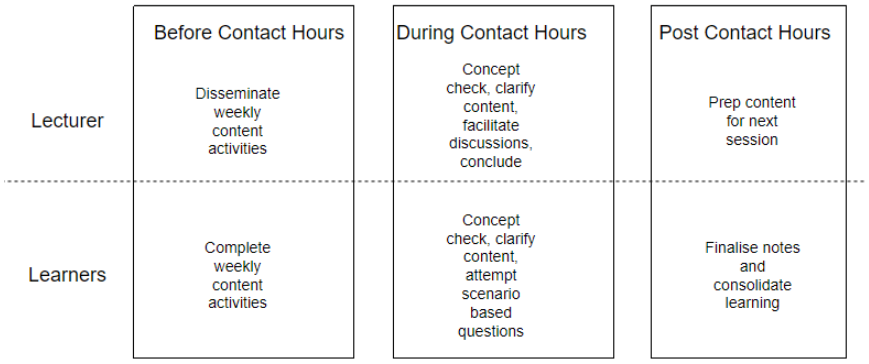

Fig. 1.1 A typical week structure for scenario-based flipped delivery

The key is that prior to engaging with the scenario-based activities, the learner should have had the opportunity to explore the related content. The lecturer should make clear to learners how the typical week works, including tasks per week and when they should engage with them. It can also be helpful to present the reasoning behind the approach, as well as giving students an opportunity to ask questions about the structure or how to complete activities they may not be familiar with. Since this is important to set expectations, it is recommended this is covered in the first contact hour with students. This means in the first week one would not expect students to have completed any engagement activities prior to attending. However, in

the following weeks students should become more comfortable with the consistent structure.

Aspects the lecturer may also wish to highlight in the initial session is how long content activities should take on average per week, any other expected behaviour such as taking notes, how to get clarification on module content, and an overview of the learning objectives, weekly content and tasks, and assessment structure and deadlines.

It is important to note that using a different mode of delivery can be challenging. In particular, a number of students feel uncomfortable with this approach as it is unfamiliar. Due to the nature of the structure, there are also areas for which there is no single acceptable answer. This can also be unfamiliar for students who may be more comfortable with coding exercises where there is less room for interpretation.

To aim to address these aspects, it is important to clearly define the structure and reasoning for the format of the module. It may be necessary to repeat this multiple times, and provide reassurance to learners that well reasoned answers are acceptable. This is of particular importance for summative assessment such as exams, where learners are more likely expect a single answer is the only solution, it is helpful to clarify that this is not true. It can also be helpful to encourage learners to speak with you directly to discuss their answers if they are unclear.

Another obstacle is the need for more self-directed learning, which can be challenging for learners who struggle to motivate themselves to engage with module content prior to SBL sessions. One option to increase motivation is to include low stakes continuous assessment, such as multiple choice quizzes. Alternatively, regular prompts and a clear list of actions required week by week can help students manage their studies more effectively.

Having decided the overall structure of the module, the next aspect to address is the facilitation of scenario-based activity sessions.

1.5.2 Facilitating Sessions

As this method is similar to a problem-based learning structure, sessions should be structured in a way which allows students to break into teams to discuss a scenario. If this is online, this can be through breakout groups. If it is in person, then depending on the room this may be more challenging, but is still possible. Sufficiently clear instructions on group choice should be provided, and it may be helpful to maintain the same groups for each week or change depending on the cohort. For example, the author's experience for undergraduate honours students is that they prefer to chose their own group, whilst Masters students typically prefer to be allocated as they have yet to make friends. A third alternative is that those who wish to chose can do so, but those who don't can abstain and be randomly allocated to a group at a defined deadline.

One challenge is facilitation is class size. This approach is generally easier to complete with a smaller class size as the lecturer can ensure all teams receive guid-

ance during the session. This is harder with larger class sizes, e.g. a class of 100 in a 50 minute session using teams of 5 would mean the lecturer would only have 2.5 minutes per team. Clearly this is sub-optimal, thus a number of adjustments are necessary to accommodate larger class sizes. To adapt, time at the start should be provided to allow students to clarify any material they may be unsure of. This means time is not required for moving around teams providing the same content clarification.

Students can also be made responsible for reporting back from these discussions. Such accountability, as noted by Duch et. al [9], gives students stronger motivation for engaging with the discussion. Groups could then be randomly chosen to report their solutions, or alternatively teams can place these in a shared document. Students are often reluctant to volunteer solutions independently when in a class setting, so it is recommended a mechanism other than simply asking the class what they achieved is used.

Guidance provided in the scenario-based activities should also be more explicit for larger class sizes. For example, a more open scenario-based activity could be broken down into smaller component parts. This would also allow the class to discuss this at each stage, rather than a single discussion at the end which may result in disengagement when given longer to discuss. Duch recommends students are given no more than 15 minutes to discuss when part of a larger class [9].

Below is an example of a scenario developed to explore user authentication.

A hospital emergency department decides to digitise their patient records. Currently patient records are paper-based, and staff carry them around the hospital as necessary. The problem is that records are being left in rooms with patients, who can clearly see them. Also, records are being lost and are not always returned to the main storage cabinet. This means in emergency situations medical staff are unable to access the records as quickly as they need to.

The current proposal is to place a computer device in each of the common areas (such as the waiting room and reception desk), as well as in each of the cubicles where patients are dealt with. The staff who need to access the records include administrators (who check patients in), nurses, and doctors. An authentication mechanism needs to be selected for the devices. Consider each of the following questions, and propose a solution given an unlimited budget. You might need to do some research to address all questions.

The prompts or questions which go along with this scenario can have more or less structure depending on the size of the class. For example, below are the prompts which could be used with a smaller class size.

- Consider the positives and negatives of different user authentication methods for this scenario and present a proposed solution with appropriate justification.

  Compare this with the prompts for a larger class as shown below.

- What should you consider when selecting an authentication mechanism for this scenario? What might the requirements be?

- What options are available for authentication?
- How does each option match your requirements?
- Given your answers to the previous questions, which option would you choose and why?
- Assume now that you have a smaller budget, what impact would this have on your choice?

Note that in the first set students are given a more open question since the lecturer can support students by giving the breakdown if needed. However, in the second set this is broken down into smaller parts to guide students since the lecturer will not be able to provide as much support to all teams. This allows the lecturer to incorporate check points where if a small number of teams are struggling, it is possible to directly address this to the whole class.

During the session, the facilitator can move between as many groups as possible within the time. It is important to try not to spend a disproportionate time with a single group. If dealing with a larger class, it may be helpful to address common issues to the class as a whole instead of repeating across multiple groups. This can be achieved in a number of ways, e.g. through a broadcast message functionality if online, or by calling the class together before splitting into groups once more.

One challenge which may occur is groups not engaging with the discussion. Depending on the year of the cohort, it may be helpful to allow learners to self select groups. By doing so, they are more likely to work with peers they are comfortable with which can help discussion. The lecturer can also prompt learners with specific questions, or ask what support they need. Of course, there is only so much one can do and so if learners do not wish to engage it may simply be helpful to explain the reasoning behind the approach and move on to another group. Should common misunderstandings or queries arise through such discussions it can be helpful to note these for reporting to the whole class.

Having completed the allocated time for discussion, it is important to bring the class back together to summarise the results. To ensure students are on track, it can be helpful to summarise possible solutions. Ideally these would be delivered by the learners themselves, however it can be challenging to get learners to volunteer solutions. To combat this, the session could be structured such that groups are be randomly selected, or a schedule for each team to present solutions could be used.

There can be challenges in delivery of such a session. Depending on the stage and background of learners, some may have less practice in skills such as communication. If this is the case, it can be helpful to provide a range of sources such as links to the relevant university skills support team as well as general resources on skills such as web resources.

In aiding learners in consolidating their learning after the session, a temporary summary of the discussions could be provided. This also helps support learners who may have missed a session, or who may have a different first language. The summary could be written, or audio, or a combination of audio and visual. The temporary nature is suggested as a way to help learners engage consistently throughout the module.

1.5.3 Assessment

Delivery of assessment with the scenario-based learning structure is similar to normal delivery, however if the assessment uses a scenario then it can be helpful to discuss an example in a session. For instance if an assessment involves completing penetration testing and a reflective video presentation for a defined client, it can be helpful to show examples and discuss as a class what was done well and what could be improved. This can help learners understand how a marking rubric can be applied to the final product.

If using an exam which asks scenario-based questions, it can be helpful to provide an example of an exam question. As discussed previously, by design the scenario-based questions in an unseen written exam are generally more precise. Also, as the questions have marks allocated to them it can be helpful to give students an opportunity to see how marks are distributed. For example, it is common for learners to focus more on the definitions and to neglect the context. This means a lower level of attainment as the structure is specifically designed to assess application of theory to a novel context. As such it can be helpful to highlight a 'strong' response indicating where marks are earned and the importance of application to the given context.

For learners with English as a second or further language, this can also be a cause for stress. Learners can struggle with the combination of terminology as well as the language for contexts. To support learners with this challenge, it can be helpful to build a glossary of both terminology as well as the types of context used.

Having covered the approach to designing and running a module which uses SBL as a mode of delivery, it is important to consider some of the challenges which have arisen in the author's experience. Firstly, it is common that a number of students feel uncomfortable with this approach as it is unfamiliar. Due to the nature of the structure, there are also areas for which there is no single acceptable answer. This can also be unfamiliar for students.

To aim to address these aspects, it is important to clearly define the structure and reasoning for the format of the module. It may be necessary to repeat this multiple times, and provide reassurance to learners that well reasoned answers are acceptable. In particular for exams, where learners are more likely expect a single answer is the only solution, it is helpful to clarify that this is not true. It can also be helpful to encourage learners to speak with you directly to discuss their answers if they are unclear.

Another challenge is the need for more self-directed learning, which can be challenging for learners who struggle to motivate themselves to engage with module content prior to SBL sessions. One option to increase motivation is to include small continuous assessment, such as low stakes multiple choice quizzes. Alternatively, regular prompts and a clear list of actions required week by week.

1.6 Conclusion

Throughout this chapter we have explored scenario-based learning as one approach to help bridge the gap between theory and application of cyber security to unknown contexts. A case study was presented to illustrate how one can design and implement a cyber security module using this approach. We have also discussed some of the challenges which can arise in the delivery of such a module, including learners discomfort with a new approach and ensuring engagement for optimal performance.

It is helpful to remember that although this chapter represents the process for a complete module design, elements of scenario-based learning can be implemented in much smaller way. For example, taking a particular topic which lends itself to this and applying SBL for that topic. It can also be built up over time, e.g. incrementally applying to a variety of topics until an appropriate level is reached. The hope is that as the reader you are now aware of the possibilities, and may decide to implement this in your own security modules, even in a small way.

References

1. Lave, J., Wenger, E. (1991). Situated Learning: Legitimate Peripheral Participation (Learning in Doing: Social, Cognitive and Computational Perspectives). Cambridge: Cambridge University Press. doi:10.1017/CBO9780511815355
2. S. Naidu, M. Menon, C. Gunawardena, D. Lekamge, S. Karaunanayaka (2007). How Scenario-Based Learning Can Engender Reflective Practice in Distance Education in Finding online voice: Stories Told by Experienced Online Educators, Chapter 4
3. F. B. Schneider, "Cybersecurity Education in Universities," in IEEE Security & Privacy, vol. 11, no. 4, pp. 3-4, July-Aug. 2013, doi: 10.1109/MSP.2013.84
4. Clark, Ruth C..,Mayer,Richard E..Scenario-based E-Learning: Evidence-Based Guidelines for Online Workforce Learning. Germany: Wiley, 2012.
5. Mio, Cristina and Ventura-Medina, Esther and Joao, Elsa (2019) Scenario-based eLearning to promote active learning in large cohorts -Students' perspective. Computer Applications in Engineering Education , 27 (4). pp. 894-909. ISSN 1099-0542 10.1002/cae.22123
6. Rankin, W. (2016) "Formal" Learning. [online] Unfold Learning. Available at: https://unfoldlearning.net/2016/12/09/formal-learning/ [Accessed 10 February 2022]
7. Baker, J. W. 2000. The "classroom flip": Using web course management tools to become the guide by the side. 11th International Conference on College Teaching and Learning, Jacksonville, FL.
8. King, Alison. "From Sage on the Stage to Guide on the Side." College Teaching, vol. 41, no. 1, Taylor & Francis, Ltd., 1993, pp. 30–35, http://www.jstor.org/stable/27558571
9. Duch, B. J., Groh, S. E, & Allen, D. E. (Eds.). (2001). The power of problem-based learning. Sterling, VA: Stylus
10. Wolfe, A. D. Using a Business Compromise Scenario to Teach Cybersecurity, Innovations in Cybersecurity Education, 157–177, https://doi.org/10.1007/978-3-030-50244-7_9
11. Dolog, P., Thomsen, L. L., & Thomsen, B. (2016). Assessing problem-based learning in a software engineering curriculum using Bloom's Taxonomy and the IEEE software engineering body of knowledge. ACM Transactions on Computing Education, 16(3), 1–41. https://doi.org/10.1145/2845091

12. Shivapurkar, Mandar, Sajal Bhatia, and Irfan Ahmed. "Problem-based Learning for Cybersecurity Education." In Journal of The Colloquium for Information Systems Security Education, vol. 7, no. 1, pp. 6-6. 2020.
13. Tom Crick, James H. Davenport, Alastair Irons, and Tom Prickett. 2019. A UK Case Study on Cybersecurity Education and Accreditation. In 2019 IEEE Frontiers in Education Conference (FIE). IEEE Press, 1–9. DOI:https://doi.org/10.1109/FIE43999.2019.9028407
14. Honebein, Peter C. "Seven goals for the design of constructivist learning environments." Constructivist learning environments: Case studies in instructional design (1996): 11-24.
15. Simone E. Volet, Modelling and coaching of relevant metacognitive strategies for enhancing university students' learning, Learning and Instruction, Volume 1, Issue 4, 1991, Pages 319-336, ISSN 0959-4752, https://doi.org/10.1016/0959-4752(91)90012-W.
16. Gagnon, George W.,and Collay,Michelle, Constructivist Learning Design: Key Questions for Teaching to Standards. United States,SAGE Publications, 2005.
17. Ben-Ari, M. Constructivism in computer science education. SIGCSE Bulletin (Association for Computing Machinery, Special Interest Group on Computer Science Education), 30(1), 257–261, 1998, https://doi.org/10.1145/274790.274308
18. Barrows, H. S.. Problem-based learning in medicine and beyond: A brief overview. In Wilkerson, L., Gijselaers, W. H. (Eds.), Bring problem-based learning to higher education: Theory and practice (pp. 3–12). San Francisco: Jossey-Bass, 1996
19. Moust, J. H. C., Van Berkel, H. J. M., & Schmidt, H. G. (2005). Signs of erosion: Reflections on three decades of problem-based learning at Maastricht University. Higher Education, 50(4), 665–683. https://doi.org/10.1007/s10734-004-6371-z
20. Anderson, Lorin W., David R. Krathwohl, and Benjamin S. Bloom. A Taxonomy for Learning, Teaching, and Assessing : A Revision of Bloom's Taxonomy of Educational Objectives. Abridged ed. 2001
21. Bloom, B. S., Englehart, M. D., Furst, E. J., Hill, W. H., & Krathwohl, D. R. (1956). The Taxonomy of educational objectives, handbook I: The Cognitive domain. New York: David McKay Co., Inc.
22. Cybersecurity Ventures (2021), Cybersecurity Jobs Report, https://cybersecurityventures.com/jobs/
23. Cyber Law Masters, Northumbria University, Accessed March 2022, https://www.northumbria.ac.uk/study-at-northumbria/courses/master-of-laws-law-cyber-law-newcastle-dtflcb6/
24. Global Security Masters, University of Glasgow, Accessed March 2022, https://www.gla.ac.uk/postgraduate/taught/globalsecurity/
25. Cybercrime Masters, University of Portsmouth, Accessed March 2022, https://www.port.ac.uk/study/courses/msc-cybercrime#careers-and-opportunities
26. What the student does: teaching for enhanced learning, John Biggs, 1999,Higher Education Research & Development, 18(1), 57-75
27. The Cyber Security Knowledge Exchange project, Edge Hill University, https://www.cyberedge.uk/cske/index.php, Accessed March 2022
28. Bada, S. O. (2015). Constructivism Learning Theory: A Paradigm for Teaching and Learning. Journal of Research Method in Education, 5, 66-70.