An Argument for Game Balance: Improving student engagement by matching difficulty level with learner readiness

Portia Pusey, National CyberWatch Center    David Tobey, Sr., Indiana University South Bend
Ralph Soule, Naval Sea Systems Command

Abstract

The exponential growth of students participating in cybersecurity competition and challenge programs has been used as support for claims that the numbers of students interested in pursuing cybersecurity careers are also increasing. However, one recent study documented a decline in novice participants over the course of three cybersecurity competitions. This paper presents an argument for supporting learner engagement by balancing the difficulty level of the game’s activities with the learner’s abilities.

1. Introduction

The time has come to add gaming slang such as OP, nerf, 2EZ, 2M2H, and pwned to the pedagogical lexicon of gaming in education. Gee, a researcher with extensive experience in games and learning asserts that “good games” can be “good learning” (2003, 2005, 2007, & 2009). However, bad games can drive players away because easy games leave players bored, while games that are too hard are frustrating (Csikszentmihali, 1990; Prensky, 2001). Fundamentally, games are “problem solving spaces that use continual learning and provide pathways to mastery though entertainment and pleasure” (Gee, 2009, p. 67).

The difficulty in game design, and we would argue in gaming in education, is to provide pathways to mastery where the challenges are just within reach of a learner’s ability to solve them so that competition activities remain “pleasantly frustrating” for the learner (Gee, 2005). However, “pleasantly frustrating” is difficult to achieve when one considers the broad range of possible abilities of the players or learners. Matching the difficulty level of the competition activities with a learner’s abilities is what we mean by game balance for gaming in education. This paper presents an argument for supporting learner engagement in cybersecurity competitions by balancing the difficulty level of the game’s activities with the learner’s abilities.

2. Cybersecurity Competitions

The US Cyber Challenge review of cybersecurity competitions notes that many of the competitions provide an environment that assesses a moderate to high number of unique, advanced skills and do a good job of providing networking and employment opportunities (The Center for Internet Security, 2011). Anecdotally, the body of literature reports that cybersecurity competitions provide students opportunities to practice their skills and participate as a member of a team (Conklin, 2005).

Learning theory suggests that cybersecurity competitions when used in education can be a scaffold where novice and non-dominant groups collaborate to learn and develop their professional identities. “Learning is recognized as a social phenomenon constituted in the experienced, lived-in world, through legitimate peripheral participation in ongoing social practice; the process of changing knowledgeable skill is subsumed in processes of changing identity in and through membership in a community of practitioners; and mastery is an organizational, relational characteristic of communities of practice” (Lave, 1991, p. 64).

Qualitative studies describe that competitions support problem-based learning with authentic situations and can be motivating and promote knowledge development (Rosembloom, 2009; Wirt, 2012). Other findings regarding STEM competitions suggest that they could develop greater interest and enthusiasm among participants in topics related to competition (Lawrence, 2004; Mansaur, 2000; Tenable Security, 2011); provide students with the opportunity to apply knowledge from curriculum to real-world problems (Carter et al., 2008; Carter et al., 2011; Kearse & Hardnet, 2008; Pastor et al, 2008; Schweitzer et al., 2009), promote differentiation and enrichment of curriculum (Schaeter, 2011; Campell, 2002), and encourage the development of teamwork and communication skills (Bowring, 2011; Carter et al., 2008; Carter et al., 2011; Kearse & Hardnet, 2008). Furthermore, competitions provide promotional opportunities for the field, career and educational institutions (Carter et al., 2008; Carter et al., 2011; Campell, 2002).

However, there is an absence of empirical studies of the effectiveness of cybersecurity competitions, which are critically needed if competitions are to be used in educational settings. Support for claims that cybersecurity competitions address the career pipeline is also lacking;
and evidence of increased interest in STEM careers from other related fields such as computer science and mathematics competitions have been not conclusive, or in many cases contradictory (Dede, 2009; Dede & Barah, 2009; Dede et al., 2005; Prenzel, 1992).

Schepens et al. (2002) assert that hands-on activities in the form of immersive educational simulations engage the learner, facilitate situational learning, and support the transfer of skills to everyday applications. Important longitudinal research on Science Olympiad success significantly correlates stronger proficiencies with the number of previous Science Olympiads attended and the number of relevant courses completed (Baird, et al., 1989). This suggests that learner capability and experience may be a factor in the success of cybersecurity competitions to engage learners and support the career pipeline. Potential cognitive and motivational effects were studied in a meta-analysis of serious games (Wouters et al., 2013). This study reported that there were no benefits to learning from using a serious game among students who were still in the process of developing foundational knowledge using drill and practice methods.

Furthermore, Cooper (2009) also found that a participant’s level of ability may be a factor in engagement. This study reported that when ability is already high, participation in an immersive education simulation tool may increase engagement. Yet, this may not be true of novice learners. A recent exploratory study of a cybersecurity tournament, which consisted of three competitions over several months, reported that there was a substantial drop-off in novice participants across the three events (Tobey, Pusey & Burley, 2014). This may suggest that engagement or career interest may decline when a competitor (learner) does not perform up to their expectations, or performs poorly relative to other competitors (learners).

The implications of these studies for cybersecurity competitions used in educational settings are manifest. If, as these studies suggest, competitions increase engagement and are effective for students with high ability, the consequence is a learning experience which will only enhance the interest of those without need (or minimal need) of an instructional intervention. Therefore, it is critical that educators consider student capabilities when planning for educational competitions. These studies suggest that matching the competition activities with the existing skill sets of the students will provide for greater engagement and perhaps learning. This game balance is essential if cybersecurity competitions are to contribute to growth in learner capabilities, engagement and increasing the pipeline to cybersecurity careers.

3. Competence Development

Cybersecurity competitions, and those involved in cybersecurity professions, measure success based on an individual’s competence (Tobey et al., 2012). This is a challenge for educators because research shows that competence-based professions, including healthcare, accounting and aviation, struggle with identifying and defining key competencies and the competencies of experts (Tobey, et al., 2012, Smith, et al. 2014). The competencies of experts are vastly different between beginners and experts. Moreover, there is a continuum of competencies between the beginners and experts which requires that instructional strategies change as a learner’s capability increases (Ericsson 2008 & 2009).

Since learning curves are steep in competence-based professions, knowing a learner’s current capabilities informs the unique instructional strategies which are appropriate for their place in the beginner-expert competency continuum.

A purpose of cybersecurity competitions in education is to develop competent practitioners. The educational use of cybersecurity competitions is supported by the work of Brown, Collins and Duguid (1989) who assert that situated expertise becomes embedded through the interaction of declarative and procedural knowledge during skilled application. The key to this skilled application is diverse opportunities for practice, collaboration, and reflection which support the conversion of declarative and procedural knowledge into generalized and adaptive abilities.

The systematic process of practice, collaboration and reflection differs along the continuum of novice to expert competency. Therefore the educational experiences provided to novices, beginners and the proficient must vary as well. Prior to becoming an expert the problems presented to these developing learners must be well-defined so that the solutions can be found among established procedures and rules. An expert has developed causal models and situational awareness which enables them to solve unknown (ill-defined) problems.

The implication of the competency research on cybersecurity competitions is that the challenges, tasks, and competition activities must consider the proficiency of the competitor. This is especially critical when competitions are used in educational environments. In order to support the progression from beginner to expert, competitions need to differentiate activities to align with the problem-solving ability of the competitor (learner).

4. Learner Readiness

As an individual learns, reasons, and solves problems mental models and schemata are formed (Ifenthaler,
Mental models “provide subjective plausible explanations on the basis of restricted domain-specific information” (2010, p. 82); these change over time. The mental models form the framework for connecting pieces of information about a topic into a single conceptual unit (Ifenthaler, Masduki, & Seel, 2011). For a beginner the framework of connecting pieces of information, which forms the cognitive structure, is sparse and has few links to related concepts. However, with instruction and practice, the beginner’s cognitive structure becomes more like an expert’s with many links between associated concepts (Ifenthaler, Masduki, and Seel, 2011).

It has been suggested that it is the complex cognitive structure which enables an expert to remain focused on valuable clues to solutions in complex, chaotic situations (Fuchs, Carpenter, Carroll, & Hale, 2011). Without sufficiently complex mental models for an unfamiliar domain, beginners struggle to identify clues to potential actions to solve advanced problems (Klein and Baxter, 2009). This suggests there are developmental readiness characteristics that are necessary in order for beginners to benefit from the intensive cognitive challenges included in many cybersecurity competitions.

### 5. Game Balance

In order for competitions in education to develop competency, the competition tasks must be aligned with a learner’s abilities and readiness to solve the challenges. Formative assessment is the key to providing challenges that facilitate learning, and a key differentiation between play and games for learning. Formative assessment is used to improve teaching and learning (Bloom, 1968). For competitions in education this means evaluating students prior to, and during, the competitions to assure that the tasks are in line with their abilities and readiness, thus providing game balance.

Readiness must be evaluated across the full continuum of competence (Tobey et al., 2012). An evaluation should include measures of depth of understanding and include domain knowledge, consistency of the application of skills as well as the adaption of knowledge and skills to solve ill-defined problems (Johnsen, 2007; O’Neil et al., 2012).

Performance in educational cybersecurity competitions must be defined and measured based on a player’s (learner’s) stage of expertise development (Tobey, 2011). A formative assessment which informs game balance should involve four dimensions: 1) volatility, 2) uncertainty, 3) complexity, and 4) ambiguity, or VUCA (Chatham, 2009, Kiili, 2005, Johnsen, 2007, Wooters et al., 2013). Formative assessments that measure VUCA will indicate a learner’s position on the learning curve and will identify which the tasks, methods, and tools should be used in the competition which align with a learner’s readiness.

### 5. Conclusions

Cybersecurity competitions are serious games; they are contests of competence that seek to teach as well as engage (Garis, et al., 2002; Vogel, et al. 2006). But there is evidence that while cybersecurity competitions attract a highly engaged population, they may not support novice players. In the gaming vernacular competitions that are 2M2H (too much to handle) might leave a learner feeling pwned (like a loser). However, cybersecurity competitions which have been nerfed (made easier) might be 2EZ (too easy) for players who are OP (over powered) or experienced for the competition tasks. Therefore, we advocate for a multidimensional assessment that supports a game balance for learners of all abilities based on the four dimensions of VUCA (Johnsen, 2007).

Competitions need to prioritize game balance especially if they are to be used in educational environments. Recent studies suggest that game balance is a key factor in increase engagement and career readiness (Cooper, 2009; Tobey et al., 2012). “A good teacher challenges her students, understands their struggles, and provides needed encouragement. A [good] game provides the same level of interaction, but with the added benefit of embedded assessments a student’s progress is continually tracked” (Phillips, 2013). Furthermore, the assessments should guide adaptations to the challenges based on the current competence level of the competitor (learner). Future research should be done to determine if game balance helps to develop critical thinkers that become motivated to learn and engaged in cybersecurity careers.

### 6. References


Ifenthaler, D., Masduki, I., & Seel, N.M. (2011). The mystery of cognitive structure and how we can detect it: Tracking the development of cognitive structures over time. *Instructional Science*, 39 (1), 41-61.


