Using Social Media to Support the Learning Needs of Future IS Security Professionals

Karen Neville[1] and Ciara Heavin[2]
[1]Business Information Systems, University College Cork, Ireland
[2]Business Information Systems, University College Cork, Ireland
KarenNeville@UCC.ie

Abstract: The emergence of social media has forced educators to think differently about the way learning occurs. Students and practitioners alike are using new technologies to connect with peers/colleagues, share ideas, resources and experiences for extracurricular activities. The social business gaming platform considered in this study leverages the social networking concept (an activity that all students actively participate in) in an academic environment. The primary objective of this technology is to foster a sense of 'thinking outside the box' and analytical ability through a medium that is widely accepted by students and graduates who have entered the workplace. Both the environment and problems are developed to adapt to suit any academic course from conducting research to proposing business solutions. This study was undertaken in order to develop information systems security (ISS) skillsets through the creation and facilitation of social business gaming, which allowed students to measure their performances of understanding as part of their on-going learning. The online business game required students to apply what they have learned to problem situations and to further develop their understanding of ISS topics. The problems posed required that the learners had to prove that they understood the material being taught in the traditional lecture and could apply what they had learned in an online environment. The on-going assessment component of the gaming network was used not just as an assessment for grades but also as a learning tool. This research focuses on a group of final year undergraduate students completing Bachelor of Science in Information Systems (IS). The online social game was utilised as part of the continual assessment process to evaluate group interaction, role-playing, competition and learning in an ISS assignment.

Keywords: social media technology, social business gaming, digital game-based learning (DGBL), information systems (IS), information systems security (ISS) and student assessment and learning.

1. Introduction

Organisations actively use simulated environments to both test (e.g. psychometric) and train (e.g. virtual trading of stocks and case study analysis) employees. Indeed, research contends that digital game-based learning (DGBL) is effective and has a place as a learning tool in modern educational environments (Kili, 2005; Van Eck, 2006). In an educational context, third level institutions utilise simulations to educate doctors and dentists but to date social gaming has not been widely applied as a learning aid for business and IS (security) graduates. With the emergence of social media and mobile technologies, the nature of the traditional "workplace" has been given new meaning. No longer is the working domain bounded by the physical constraints of tangible office settings. Increasingly knowledge exchange, idea generation and decision-making occur in the "workspace" enabled by widely accepted social media technologies. Consequently, it is imperative that educators leverage "workspace technologies" such as Facebook, Twitter and Second Life in a constructive way beyond their more typical informal social use. This may be done to further develop the skillsets acquired by students through the traditional channels, essentially promoting the use of technologies that they will be required to utilise as qualified business and IS graduates.

Van Eck (2006) considers the complexity of understanding DGBL, the number of variables, constructs and the gaming environment. This study endeavours to move beyond a tightly controlled experiment to explore social media technology and how it may be leveraged to enhance and support the learning and assessment mechanisms utilised in an undergraduate, final year, IS security module. The objective of this research was motivated by the importance of providing students with a practical proactive knowledge of the implementation and management of IS security in business. Students learn how to, through the combination of a flexible social learning environment and role-playing, proactively plan, defend and attack a business. The online ISS knowledge environment used in this study adhered to an on-going assessment process, which clearly outlined the criteria of the game allowing students to both collaborate and compete against their peers in a series of challenges.

The subsequent section considers the area of learning, focusing on the weaknesses associated with traditional learning and highlighting how eLearning tools specifically social media technology may

Reference this paper as: Neville, K and Heavin, C. "Using Social Media to Support the Learning Needs of Future IS Security Professionals" *The Electronic Journal of e-Learning* Volume 11 Issue 1 2013, (pp29-38), available online at www.ejel.org

overcome many of these. Following this, the nature of ISS education is presented. The research approach is then outlined. The case is presented and discussed and finally attention is given to the conclusions of the study.

2. Theoretical foundation

The web offers unparalleled opportunities to education (Mioduser *et al*., 1999). The intensity of competition in the business market, advances in technology, and a strong shift towards a knowledge-based economy have each contributed to the demand for virtual learning environments (VLE) (Neville *et al.* 2009). According to Watson *et al.* (2007) research regarding the use of educational technology continues to be important because of the pace at which technology is being incorporated into academic curricula. While originally created for distance education, VLEs are now most often used to supplement traditional face to face classroom activities, commonly known as blended learning. E-learning supports both the learner and the educator in a number of ways, for example, differing learning styles can be catered for, which help educators reach more students in varied ways, and enable more students to learn the course material (Sulcic and Lesjak, 2001). If an organization or university does undertake an e-learning initiative they must develop an effective solution that recognizes the need for good learning practices, which incorporates good design and development guidelines (Sulcic and Lesjak, 2001). The learning dimensions advocated by Reeves and Reeves (1997) and Neville *et al.* (2005) for interactive learning and collaboration should be incorporated into the design of any learning environment. The dimensions, as follows, describe the characteristics of a learning environment (1): educational philosophy: which (2): learning theory, (3): goal orientation, (4): task orientation, (5): source of motivation, (6): role of the teacher, (7): metacognitive support, (8): collaborative learning, (9): cultural sensitivity and (10): structural flexibility.

Active learning approaches, such as case-based learning and problem-solving, have long been advocated as ways of fostering deeper learning (Healy and Neville, 2009; Boyce *et al.* 2001; Biggs, 1994) as well as an effective means of motivating learners (Papastergiou, 2008). For many years organisations have been using problem-solving scenarios such as business simulations to both test and train employees. Simulations enhance the learner's logical reasoning, numeric abilities and spatial thinking through real world problem-solving scenarios. Realising the potential of such methods however requires active engagement from educators and learners alike (Baskerville, 2008; Healy and McCutcheon, 2008). For many educators, the lack of appropriate materials, learning management, assessment techniques and guidance are often perceived as barriers to student or employee engagement. In order to overcome these limitations VLEs are increasingly utilised beyond the realm of distance education *"but are now in common use in traditional, campus-based institutions, supporting 'mixed mode' provision of learning resources and support"* (Keller, 2005, p300). With the 'right' underlying pedagogical approach, social media technology provides educators with the technical platform to overcome these well-cited issues, providing third levels educators with a media to provide a more complete learning experience.

2.1 Social media in learning

Social media provides new opportunities for innovating and modernising Education and Training institutions and for preparing learners for the 21st century (Redecker et al., 2009). Furthermore, social media technologies have the potential to support and enhance teaching and learning in higher education (Ajjan and Hartshorne, 2008) providing learners with a chance to manipulate their learning environment and to participate actively in the learning process (Hrastinski, 2009). Up to recently, Web 2.0 technologies have largely applied only in a social sphere; however a growing number of businesses are adopting enterprise social software technologies. It is through these collaborative technologies that students and knowledge workers will gain enhanced insight in the knowledge at their disposal. These tools will also enable information workers to locate and connect people with certain expertise across organizations, bringing people, systems and data into alignment faster to respond to challenges and take advantage of competitive opportunities.

In an educational context Chen and Bryer (2012, p99) state that *"publicly open social media sites provide students with access to more information and experiences than they would get in a closed environment alone. If properly facilitated and framed, such expanded exposures can benefit student learning by creating more connections across boundaries and over time".* Valjataga and Fielder (2009, p58) widely support the use of social media technology as a means of skilling students in preparation for the 'real world', "*in order to be able to cope with many authentic challenges in* *increasingly networked and technologically mediated life we need to construct opportunities for participants in higher educational settings to practice the advancement of self-directing intentional learning projects."* Research conducted by the Institute for Prospective Technological Studies (IPST) (Redecker et al., 2010) summarise the advantages of social media in learning through the 4 C's 1) Content – social media technology facilitates access to a wide variety of freely available content, 2) Create – allows users the freedom to create their own digital content, 3) Connect- connecting learners to one another as well as to experts and teachers and 4) Collaboration- supports collaboration amongst learners and teachers in a particular project of subject areas (Redecker et al., 2010). However, Selwyn (2007) indicates that research is needed in the area of education, and their use of social media applications as online learning environments, and the learning affordances they may offer.

2.2 IS security education

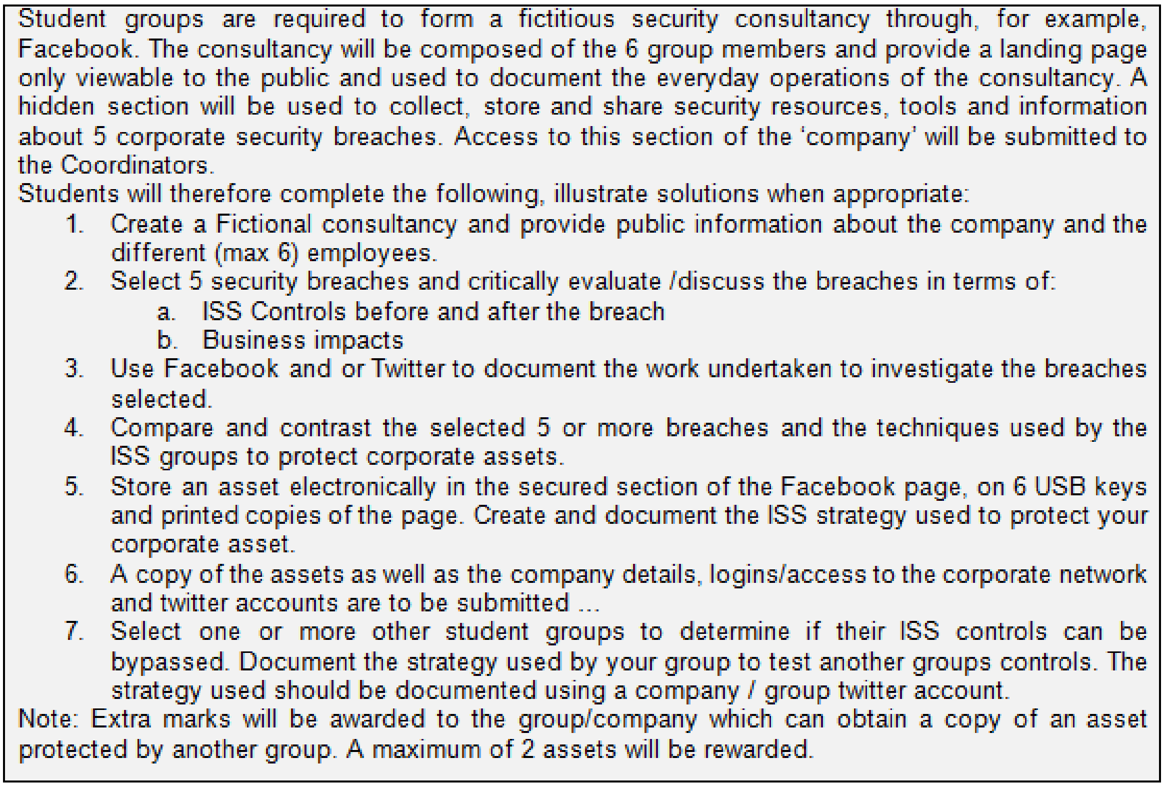
In just a few decades, the use of IS has formalised information management and streamlined the administration of organisations (Galliers and Newell, 2001; Dhillon, 2006). One of the fundamental problems regarding ISS is for an organisation to choose the right kind of environment to function in. Strategic ISS issues relate to where the firm chooses to operate and the scope of the organisation's relationship with other organisations. Investment in IS Security has increased, but so have the number and range of security breaches (CSI, 2009). While many organisations have engaged in identifying security issues and as a result developed appropriate IS Security policies, there is a clear mismatch between policies and what is done in practice. Researchers have termed this as a gap: in espoused theory (actions that people write) and theory-in-use (what people actually do). Therefore theories-in-use have degrees of effectiveness which are learned (Mattia and Dhillon, 2003). Espoused theory and theory-in-use are a part of the double-loop learning concept which creates a mindset that consciously seeks out security problems in order to resolve them. This results in changing the underlying governing variables, policies and assumptions of either the individual practitioner, function or the organisation. Considering the complexity of the subject area, it is evident that teaching the know-how and know-what of an ISS course to IS undergraduates requires a hands-on approach to adequately deal with some of the concepts and underlying principles. Using social media to move beyond the traditional learning environment ensures that students acquire a more complete and practical experience (Chen and Bryer, 2012), better preparing them as ISS professionals of the future.

3. Research approach

This research study outlines the adoption of a blended approach to learning by IS Security teachers / researchers within a university setting. The department facilitates a learning strategy of teaching, supporting and attracting learners. This study pursued a single case study approach, as per Darke *et al.* (1998, p281) "*a single case may provide the basis for developing explanations of why a phenomenon occurs"*. Undoubtedly, there remains a dearth of empirical research studies focused on the use of social media technology to support teaching and assessment in third level IS education. In light of this, Darke *et al*. (1998) claim that in areas within IS, where theory and understanding are not well developed, case study research is most appropriate. The case study selected for this research study was the IS department within University College Cork (UCC), Ireland. The IS department was selected because it is the primary group within the university to develop, customize and blend traditional learning approaches and eLearning technologies, this is reflective of the nature of IS disciplinary emphasis on people, process and technology, providing students with a complete learning and evaluation experience. The researchers examined the implementation of an online game designed to allow students leverage their classroom acquired know-what in the area of IS security in a simulated 'real world' environment, social media technology (Facebook). Table 1 provides a description of the game distributed to a class of 72 IS undergraduate students.

The authors investigated the degree to which the benefits of the game met the learning needs of the students. The analysis also expanded the on-going design of the game to provide an innovative approach to learner support that is more akin to the true essence of social learning. Figure 2 illustrates and Table 2 outlines the content developed to support the learners' requirements, as determined through ongoing discussions and discussions with ISS professionals and reviews of current ISS literature. The objective of this study was twofold; it enhanced the students learning experience by enabling them to use theoretical ISS concepts in a practical way while facilitating their interaction with other learners. Secondly, this learning experience contributed to student's preparation for their future careers as IS graduates in a workplace that is increasingly reliant on these types of technologies. The next sections provide a description of the ISS module and the social game. This is followed by the results of the student's participation and an analysis of the results.

Table 1: ISS game description



Student groups are required to form a fictitious security consultancy through, for example, Facebook. The consultancy will be composed of the 6 group members and provide a landing page only viewable to the public and used to document the everyday operations of the consultancy. A hidden section will be used to collect, store and share security resources, tools and information about 5 corporate security breaches. Access to this section of the 'company' will be submitted to the Coordinators.

Students will therefore complete the following, illustrate solutions when appropriate:

1. Create a Fictional consultancy and provide public information about the company and the different (max 6) employees.
2. Select 5 security breaches and critically evaluate /discuss the breaches in terms of:
   a. ISS Controls before and after the breach
   b. Business impacts
3. Use Facebook and or Twitter to document the work undertaken to investigate the breaches selected.
4. Compare and contrast the selected 5 or more breaches and the techniques used by the ISS groups to protect corporate assets.
5. Store an asset electronically in the secured section of the Facebook page, on 6 USB keys and printed copies of the page. Create and document the ISS strategy used to protect your corporate asset.
6. A copy of the assets as well as the company details, logins/access to the corporate network and twitter accounts are to be submitted ...
7. Select one or more other student groups to determine if their ISS controls can be bypassed. Document the strategy used by your group to test another groups controls. The strategy used should be documented using a company / group twitter account.

Note: Extra marks will be awarded to the group/company which can obtain a copy of an asset protected by another group. A maximum of 2 assets will be rewarded.

4. Background to the study - social gaming environment

Problem-solving skills require the use of a number of different learning strategies and types of knowledge. The learner's own experience, internal mental models, and other 'cognitive structures' are necessary to'construct' their own knowledge when faced with new information or different situations. The game was created to facilitate and support understanding and learning of the links between ISS and its business applications. The creation of fictitious companies and corporate espionage components presented students with the opportunity to play the role of ISS practitioners protecting and simultaneously targeting corporate boundaries in an attempt to acquire and protect assets. This component proved very helpful in developing a corporate ISS strategy as the groups had to consider potential attacks to try and steal another group's secret.

At the start of the teaching period, the class (72 students) is divided into teams of 6 members. We ask for volunteer team leaders at the first class meeting; then once each class member has introduced themselves the team leaders take it in turns to select team members. Each group is expected to meet at least once a week. Project Teams are asked to record minutes of all meetings and day-to-day operations through Twitter and these must be kept for review by the co-ordinators throughout the year (protected Tweets with group and coordinator access). Facebook and Twitter are both used to co-ordinate the work effort; thus planning of ISS tasks and workloads well in advance will form an essential element of the overall assignment.

The game is structured as part of the lecture series (24*2 hours) to gradually build knowledge of the ISS subject domains while simultaneously simulating 'real world' situations when the groups are asked to deliver a series of requirements to determine their level of understanding of the topics (Table 2) discussed in class. At the end of each assessment submission the goals for the next submission and lecture are set, based on the level of knowledge and understanding demonstrated by students up to that point. Groups submit and present their deliverables at agreed deadlines, this is a significant indicator of the understanding (or the lack thereof) achieved by the individual groups at each stage. This enables a post- mortem evaluation approach (Kasi et al., 2008).

Table 2: Topics taught and game outcomes

Objective	Performances	Assessment	Outcomes
How do you address ISS business problems?	Students will understand how to identify assets & allocate the right controls	Related exercises of case organizations	Analysis of Real cases & solutions used to protect assets
How do you identify the ISS requirements of a business?	Students will see the connection between ISS controls & business value	Provide the requirements of a business case	Business impacts of security breaches will be measured.
How should you address analysis requirements?	Students will understand how to analyse problems	Illustrate a logical view of a solution	ISS strategies are selected, discussed & evaluated
How can you use what you have learned to build a solution?	Students will understand the building blocks of an ISS solution	Provide step-by-step guide incorporating a Security life cycle	ISS plan developed
How do you use solve a security breach?	Students will address business & ISS threats, controls & disaster recovery	Provide a fake solution to a security breach based on a case description	Computer forensics of a breach presented
How do you use build an ISS report & apply lessons learned?	Students will understand the skills necessary to convey technical ISS issues to mixed audiences	Feedback on presenting lessons learned from case assessments	Audit review conducted of a selected case
Understanding			
Goals	How to:		
Students will understand the process of 'Forming fictitious ISS companies'.	Submit Company through Facebook , roles, Twitter diary & asset	Emailed to Lecturer early in Term 1	Details of Company, Structure & secret submitted
Students will understand how to apply a divide & conquer approach to an ISS problem	Develop a strategy to protect the group asset. Target other groups to obtain their asset	Presentation through a preliminary report & reported through protected tweets.	Full ISS solution submitted for review & feedback
Students will understand how to develop ISS strategies to protect corporate boundaries	Present a walkthrough of the key elements of their strategies: failures & successes	Presentation of solution, with detailed feedback provided	ISS solution presented & reviewed
Students will learn to compete against their peers through ISS bypass attempts.	Students will understand the complete process of protecting & targeting an organization	Construction & presentation of the final versions of solutions.	ISS solution tested internally & externally (penetration tests).

An evaluation of published ISS breaches is also a requirement of the game. Groups are required to select 5 security breaches and critically evaluate /discuss the breaches in terms of the controls used before and after the breach. The business impacts are also investigated. These evaluations are then presented and discussed in class. In some instances 3 or 4 groups would have investigated the same case. However each had their own view regarding how the company reacted to and learned from a reported (published) incident. This often resulted in discussions and proposals of what should have been the course of action adopted by the case. Case analysis and discussion is a traditional form of an in-class exercise. This component was enhanced through the use of social media to store documents (reports, articles, videos and slides) and Twitter searches using # to find the discussions which occurred in real-time regarding, for example, the Sony1[1] or RSA2[2] attacks. The topics covered through the ISS business game/teaching case included: analysing ISS requirements; developing ISS strategies; creating ISS plans; ISS controls, Computer Forensics, Compliance, SecSDLC (systems development life-cycle); Secure Development, Designing Audit reporting and project management. This theory was selected and delivered according to academic and practitioner research. Table 2 outlines the how these topics were taught, applied and assessed through the ISS business game.

[1] http://www.informationweek.com/news/security/attacks/229402362
[2] http://www.informationweek.com/news/security/attacks/229301337

Enhancing the Teaching and Learning Process for ISS Students

Student groups submitted their secret / assets at the beginning of the game (Term 1). Additionally Figure 2 was used to illustrate a sphere of possible ISS controls aligned to potential corporate assets such as: data, information and knowledge. The sphere created by the researchers / game coordinators to illustrate the integration as well as the use of different ISS controls (informal, technical and formal). Each asset is mutually interdependent and of value requiring appropriate countermeasures. They are always at risk from attacks through the employees and computer systems that have direct access to the assets or corporate secrets. The sphere was used by the groups to determine the type of protection layer, in the form of countermeasures to prevent access to the inner layer from the outer layer, was needed. Technical controls were then identified and implemented between systems and the different assets, between networks and the systems, and between the Internet and internal networks. As illustrated, a variety of controls were used to protect the data, information and knowledge stored by a group. As employees/students can directly access each ring as well as the knowledge at the core of the model, unique approaches to IS Security are required by participants. Employees/students must become safeguards, which are effectively trained, implemented, and maintained, or else they, too, become a threat to the information and knowledge stored.

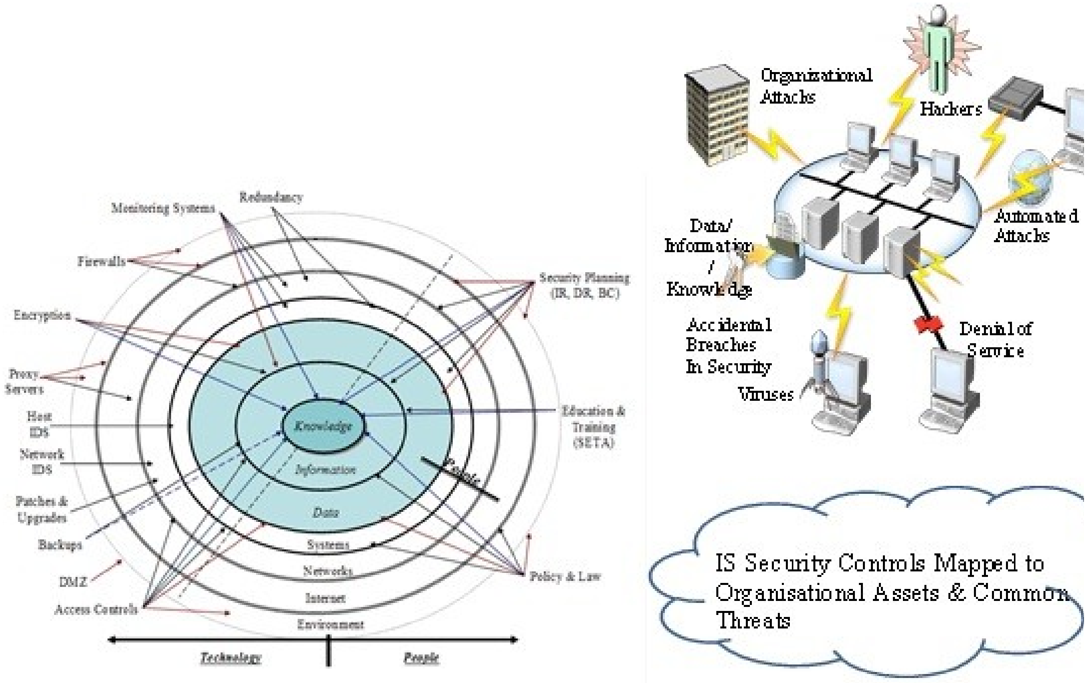
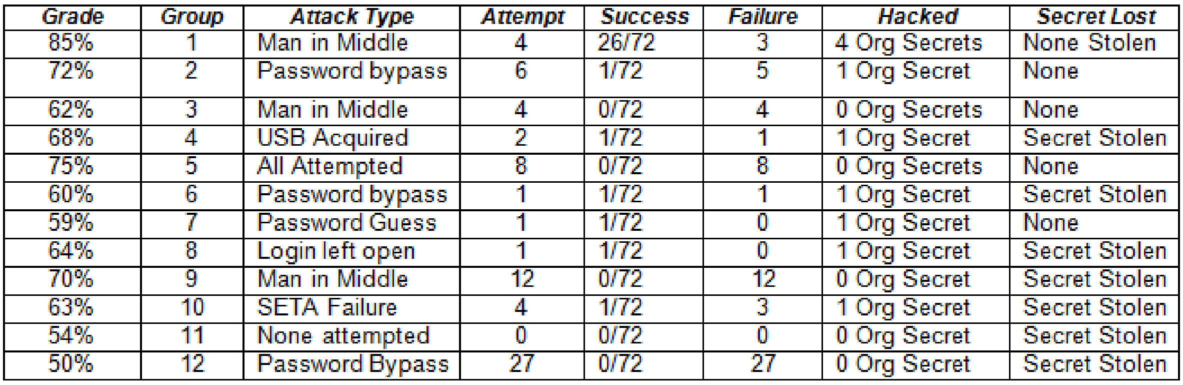


Figure 1: ISS controls and common attacks (created by the authors)

However while the same technologies, discussed in class and reviewed by the groups, empower ISS practitioners they also empower hackers and hacking organisations to subjugate different types of information systems. This threat became part of the game as students adopted the role of hackers and targeted the secret / asset of another groups to gain extra marks. Table 3 outlines the results of the hacking component of the game in the academic year 2011/2012. The groups primarily tried to use man in the middle and password bypass attacks. The most successful attack was conducted by group 1. The group emailed the class using a fake email address from one of the coordinators: Coordinator1@gmail.ucc.ie requesting that students were to email their secrets before 5pm on the day of the agreed 'secret' submission. 26 students emailed their group's secrets to the fake account. This earned group 1 two extra bonus marks due to the limit of 2 and the fact that by the time the project concluded (despite being consistently targeted by other 11 groups) did not have their corporate secret stolen. This attack was also used to illustrate well published cases of man-in-the-middle attacks. That is despite the fact that this topic was covered during class (2 weeks before the attack occurred) to the amusement of the majority of the students, due to the simplicity of the attack, 26 students fell for it. This reinforced the importance of controls such as SETA (security, education, training and awareness). As outlined in the Table 3 groups were successful in acquiring another group's asset as well as unsuccessful in protecting their own corporate assets.

Table 3: Attack Attempts (Step 7 of Table 1)



Grade	*Group*	*Attack Type*	*Attempt*	*Success*	*Failure*	*Hacked*	*Secret Lost*
85%	1	Man in Middle	4	26/72	3	4 Org Secrets	None Stolen
72%	2	Password bypass	6	1/72	5	1 Org Secret	None
62%	3	Man in Middle	4	0/72	4	0 Org Secrets	None
68%	4	USB Acquired	2	1/72	1	1 Org Secret	Secret Stolen
75%	5	All Attempted	8	0/72	8	0 Org Secrets	None
60%	6	Password bypass	1	1/72	1	1 Org Secret	Secret Stolen
59%	7	Password Guess	1	1/72	0	1 Org Secret	None
64%	8	Login left open	1	1/72	0	1 Org Secret	Secret Stolen
70%	9	Man in Middle	12	0/72	12	0 Org Secret	Secret Stolen
63%	10	SETA Failure	4	1/72	3	1 Org Secret	Secret Stolen
54%	11	None attempted	0	0/72	0	0 Org Secret	Secret Stolen
50%	12	Password Bypass	27	0/72	27	0 Org Secret	Secret Stolen

The game reinforced the need to recognise that the technical side of IS Security is a part of, but not always the answer to, the different IS Security challenges. Knowledge and expertise of the technologies necessary to alleviate IS Security risks are valuable. However ISS students must be familiar with critical business processes as well as ISS business impacts. Technological changes, in both secure hardware and software, are as constant as the increase in the number of threats to corporate IS Security. Forgetting the most basic types of attacks and the potential for employee mistakes are common issues for organisations in general. These errors were experienced by the student groups as outlined in Table 3. The mistakes made, as well as adopting the role of hacker, reinforced the material taught in class.

There is a pressing need for ISS practitioners to gain the knowledge necessary to diagnose problems, plan action and implement solutions. The game was utilised to allow students to apply the material taught in class to an environment they controlled. The use of social media enabled the students to build their own ISS solutions to potentially protect their assets and it enabled them to target another group without in any way interfering with the college network. The environment itself (Facebook and Twitter) allowed them the freedom to use a platform that was familiar, allowed shared work and access to external expertise.

5. Discussion

Research has increasingly advocated active learning strategies to enhance the effectiveness of the student learning experience (Biggs, 1994; Boyce et al., 2001; Ueckert and Gess-Newsome, 2008; Healy and Neville, 2009). Active learning strategies will initially challenge most students. However careful introduction can and does offer benefits even for those who were not originally technically oriented. A recent study shows that DGBL incorporated into a social network website is a feasible and sound model for teaching (Hwang, 2012). Research on the use of games as a teaching strategy indicates that the difficulties that may arise relate to the application of active learning methods, rather than with the method in and of itself (Healy and McCutcheon, 2008). Our experience of using the game presented in this study demonstrates that such difficulties such as the application of ISS theory can be overcome as students are supported to fully understand concepts and furthermore recognise the relationships among ideas (Ueckert and Gess-Newsome, 2008). Undoubtedly, this active approach engaged and motivated the groups to work with each other within the group as well as 'compete' against the other teams. Extant research supports the use of DGBL to motivate student learning (Papastergiou, 2008), in this study the feeling of competition pushed students to uncover new and interesting ways to better their classmates by trying to steal their organisational secrets. This level of engagement goes beyond the traditional methods of teaching and learning, allowing students to embrace concepts and theories that may be perceived as trivial and even boring when delivered in a classroom environment via traditional methods such as overhead projector or in class notes. In line with recent extant research in the field of DGBL (Lin, 2011; Hwang, 2012), the use of social media technology as a learning tool heightened the students' interest in the subject matter.

The emergent nature of the module content must also be recognised from the outset and viewed as an opportunity for ongoing development of the student and group's ISS understanding and skill-set. This coupled with the use of social media technology to teach and evaluate student's understanding of the material is a work in progress; this need for continual re-crafting is supported by Hemmi et al. (2009). Nonetheless, one of the key advantages of the game is its hybrid orientation towards ISS and Business. Students are forced to realize, acknowledge and understand the integration of materials taught in the module and how these may be embodied in 'real world' scenarios. The resulting skills-set developed through such activity are twofold, meeting the calls for same in both academic and professional sources (Wankel, 2010; Chan and Reich, 2007).

6. Conclusion

In their recent study Tay and Allen (2011, p153) purport that "staff (educators) saw both the necessity of including greater use of social media in teaching and, at the same time, believed that neither social media technologies themselves, nor the informal and personal cultures of use that students had developed, would necessarily mean that this innovation would – without close attention to pedagogic design – reliably improve students' outcomes." Certainly, while social media technology has proven to positively enhance the student learning experience, it is imperative that academia continues to -

- ***Engage*** with social media technologies in order to further understand and leverage their capabilities
- ***Ensure*** that this convergence of the traditional and new provides students with a fulfilling learning experience
- ***Adapt*** to the changing needs of industry specifically focusing on developing students' competitive skill-sets, preparing them for the challenges of the workplace

Unquestionably, Information and knowledge work is no longer confined to a small elite group of highly educated and specialized experts (Schön, 1995). Certainly, the most important changes driving knowledge and information workplaces are the evolutionary responses to the major demographical, technological, social and economic shifts in society and the rise of the internet based Knowledge Worker. Companies and universities face daunting challenges as they compete for the best talent. They face a diminishing demographic of young workers entering a multigenerational workplace. They will need to attract new talent, train, retain and create an engaged workforce. Workers will need to work longer in their lifetime than preceding generations. Workers will mainly be Knowledge Workers, utilizing the internet, computer technology and communications technology, and being assisted by knowledge processing platforms for their work. Working in physical office spaces with colleagues will diminish, giving way to virtualized teams in distant geographical locations. Employers will have to equip their employees with the best in connectivity tools where necessary to replace the lack of face-to-face communication. Organizational leaders are keenly aware that the workplace is changing and are already recruiting a new breed of employee. They are adapting their workplace policies and strategies to appeal to all generations. Therefore educators must adapt to the changing needs of industry and students in developing competitive skill-sets through traditional and innovative teaching approaches.

References

Ajjan, H. and Hartshorne, R. (2008) "Investigating faculty decisions to adopt Web 2.0 technologies: Theory and empirical tests", Internet and Higher Education 11, pp71-80.

Baskerville, R. (2008). Challenging the Challenge: Measure what makes you better and be better at what you Measure, European Journal of Information Systems, 17: pp. 1-3.

Banathy, B., (1994) Designing Educational Systems: Creating our future in a changing world. In C.M

Biggs, J. 1994. "Student Learning Research and Theory: Where do we Currently Stand?" *In Gibbs, G. (ed), Improving Student Learning: Theory and Practice*, Oxford: Oxford Centre for Staff Development.

Boyce, G., Williams, S, Kelly, A. and Yee, H. 2001. "Fostering Deep and Elaborative Learning and Generic (Soft) Skill Development: The Strategic Use of Case Studies in Accounting Education", *Accounting Education*, (10:1), pp. 37-60.

Chen, B. and Bryer, T. (2012) "Investigating Instructional Strategies for Using Social

Media in Formal and Informal Learning", The international Review of Research in Open and Distance Learning, 3 (1), pp87-104.

Computer Security Institute. (2009). Computer Security Issues and Trends: 2009, CSI/FBI Computer Crime and Security Survey, http://www.gosci.com, Accessed: 23/06/09.

Computer Security Institute. (2010). Computer Security Issues and Trends: 2010, CSI Computer Crime and Security Survey, http://www.gosci.com, Accessed: 25/06/10.

Cuban, L. (1993) How Teachers Taught [2nd Edition] NY: Teachers College Press.

Darke, P., Shanks, G. and Broadbent, M. (1998), "Successfully completing case study research: combining rigor, relevance and pragmatism", Information Systems Journal, (8), pp. 273-289. Dhillon, G. (2006). Principles of Information Systems Security: Texts and Cases, John Wiley and Sons Publishers.

Galliers, R.D. and Newell, S. (2001). Back to the Future: From Knowledge Management to Data Management. In Global Co-Operation in the New Millennium, The 9th European Conference on Information Systems, Bled, Slovenia, June 27-29, pp. 609-615.

Goodlad, J, (1984) A Place called school, New York : McGraw-HIll Book Co.

Hannum, W., and Briggs, L. (1982) How does instructional system design differ from traditional instruction? Educational Technology, 22[1], pp. 9-14.

Healy, M. and McCutcheon, M. 2008. "Engagement with Active Learning: Reflections on the Experiences of Irish Accounting Students". *Irish Accounting Review*, (15:1), pp.31-49.

Healy, M. and Neville, K. 2009. "A Teaching Case: Towards Bridging Disciplinary Divides in IT Education", *In Proceedings of the 17th European Conference on Information Systems* (ECIS 2009), Verona Italy.

Hemmi S. Bayne, R. Landt (2009) "The appropriation and repurposing of social technologies in higher education", *Journal of Computer Assisted Learning*, 25 (2009), pp. 19–30.

Hwang, J. (2012) "Development and Evaluation of Peer Feedback in the English Quiz Game Design in Social Network", Advanced Learning Technologies (ICALT), 2012 IEEE 12th, pp. 235 – 239.

Keller, C. (2005) "Virtual learning environments: three implementation perspectives", Learning, Media and Technology, (30), (3), pp. 299–311.

Kili, (2005) Digital game-based learning: Towards an experiential gaming model

Lee, S. Y. and Brand, J. L. (2005) Effects of control over office workspace on perceptions of the work environment and work outcomes. Journal of Environmental Psychology, 25, pp323-333.

Lin, K. (2011) "Online Interactive Game-Based Learning in High School History Education: Impact on Educational Effectiveness and Student Motivation", U-Media, 2011, pp. 265 – 268.

Mattia, A., and Dhillon, G. (2003). Applying Double Learning to Interpret Implications for Information Systems Security Design. IEEE Systems, Man and Cybernetics Conference, Washington DC.

Mioduser, D., Nachmias, R., Lahav, O. and Oren, A. (1999) "Web-based learning environments (WBLE): Current implementation and evolving trends, *Journal of Research on Computing in Education;* Fall 2000; 33, 1; Research Library, pp. 55.

Neville, K., Heavin, C., and Walsh, E. 2005. "A Case in Customizing E-Learning", *Journal of Information Technology,* (20), pp 117-129

Neville, K., Woodworth, S. and Adam, F.2009. "Enterprise Information Systems in Retail", In the Proceedings of the Decision Support Systems Conference, 2009.

Redecker, C., K. Ala-Mutka, M. Bacigalupo, A. Ferrari and Y. Punie (2009). *Learning 2.0: The Impact of Web 2.0 Innovations on Education and Training in Europe. Final Report*. JRC Scientific and Technical Report, EUR 24103 EN: http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=2899.

Redecker, C., Ala-Mutka, K. and Punie, Y. (2010) *Learning 2.0 - The Impact of Social Media on Learning in Europe*, JRC Scientific and Technical Report, http://www.ict-21.ch/com-ict/IMG/pdf/learning-2.0-EU-17pages-JRC56958.pdf

Reeves, T.C., and Reeves, P.M. 1997. "Effective Dimensions of Interactive Learning on the World Wide Web". *In B.H. Khan (Ed.), Web-Based Instruction*, pp.59-66. Englewood Cliffs, New Jersey: Educational Technology Publications, Inc.

Reigeluth, C.M (1994) Introduction: An Imperative for System Change, In C.M Reigeluth and R.J Garfinkle [Editors], Systemic Change in Education. Englewood Cliffs, NJ: Educational Technology Publications.

Papastergiou, M. (2008)"Digital Game-Based Learning in high school Computer Science education: Impact on educational effectiveness and student motivation" *Computers & Education*, Volume 52, Issue 1, January 2009, pp.1–12

Schneckenberg, D. (2009) "Web 2.0 and the empowerment of the knowledge worker", *Journal of Knowledge Management*, Vol. 13, No. 6, pp. 509-520.

Schon, D.A. (1995) "Knowinginaction: The new scholarship requires a new epistemology, *"Change*, November/December, pp.27-34.

Selwyn, N. (2007) "Web 2.0 applications as alternative environments for informal learning - a critical review" http://www.oecd.org/dataoecd/31/37/39459090.pdf, Accessed 16/5/2012

Sulcic V., and Lesjak D. 2001. "DE in Slovenia: Where are we?" *In Proceedings of the 9th European Conference on Information Systems* (ECIS 2001): "Global Co-operation in the New Millennium", pp. 1087-1097, 27th-29th June 2001, Bled, Slovenia.

Tay, E. and Allen, M. (2011) "Designing social media into university learning: technology of collaboration or collaboration for technology?", Educational Media International, Vol. 48, No. 3, September 2011, pp151–163.

Ueckert, C. and Gess-Newsome,J. (2008) *"Active Learning Strategies",* Science Teacher, (75), (9), pp.47-52.

Valjataga, T. and Fielder, S. (2009) "Supporting students to self-direct intentional learning projects with social media", *Educational Society, 12* (3), *58-69.*

Van Eck, D. (2006) "Digital Game-Based Learning: It's Not Just the Digital Natives Who Are Restless…." Educause Review, March/April, pp.17-30.

Wanberg, C. R. and Banas, J. T. (2000) Predictors and outcomes of openness to changes in a reorganizing workplace. Journal of Applied Psychology, 85, 132-142

Wankel, C. (2010) Cutting-edge social media approaches to business education: Teaching with LinkedIn, Facebook, Twitter, Second Life, and blogs. Wankel, Charles (Ed.) Marovich, Matthew (Col); Stanaityte, Jurate (Col); pp. 1-5. Charlotte, NC, US: IAP Information Age Publishing, 2010. vi, 344 pp.

Watson, S.F, Apostolou, B., Hassell, J.M and Webber, S.A. 2007. “Accounting Education Literature Review (2003-2005)”, *Journal of Accounting Education*, (25), pp.1-58.