

Regis University ePublications at Regis University

All Regis University Theses

Summer 2010

An Examination of Online Learning Security Requirements Within a Virtual Learning Environment of an Irish University

Caroline Horan

Regis University

Follow this and additional works at: <https://epublications.regis.edu/theses>



Part of the [Computer Sciences Commons](#)

Recommended Citation

Horan, Caroline, "An Examination of Online Learning Security Requirements Within a Virtual Learning Environment of an Irish University" (2010). *All Regis University Theses*. 298.

<https://epublications.regis.edu/theses/298>

This Thesis - Open Access is brought to you for free and open access by ePublications at Regis University. It has been accepted for inclusion in All Regis University Theses by an authorized administrator of ePublications at Regis University. For more information, please contact epublications@regis.edu.

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Use of the materials available in the Regis University Thesis Collection ("Collection") is limited and restricted to those users who agree to comply with the following terms of use. Regis University reserves the right to deny access to the Collection to any person who violates these terms of use or who seeks to or does alter, avoid or supersede the functional conditions, restrictions and limitations of the Collection.

The site may be used only for lawful purposes. The user is solely responsible for knowing and adhering to any and all applicable laws, rules, and regulations relating or pertaining to use of the Collection.

All content in this Collection is owned by and subject to the exclusive control of Regis University and the authors of the materials. It is available only for research purposes and may not be used in violation of copyright laws or for unlawful purposes. The materials may not be downloaded in whole or in part without permission of the copyright holder or as otherwise authorized in the "fair use" standards of the U.S. copyright laws and regulations.

**AN EXAMINATION OF ONLINE LEARNING SECURITY REQUIREMENTS
WITHIN A VIRTUAL LEARNING ENVIRONMENT OF AN IRISH UNIVERSITY**

A THESIS

SUBMITTED ON 27 OF AUGUST, 2010

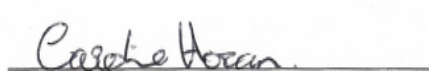
TO THE DEPARTMENT OF INFORMATION SYSTEMS

OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES

OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN
SOFTWARE AND INFORMATION SYSTEMS

BY

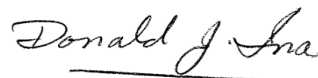


Caroline Horan

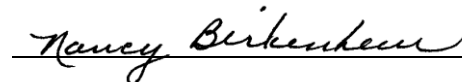
APPROVALS



Erik L Moore, Thesis Advisor



Donald J. Ina, MCT626 Facilitator



Program Coordinator

Abstract

As the adoption of e-learning and need for lifelong learning increases, it is vital the administrator of a virtual learning environment continually ensures reliable and secure data. This case study engaged in the initial steps of analysing the use and security needs of a virtual learning service within a university of Ireland. The university provided two virtual learning services which were comparatively analysed, from a security and data protection perspective. In addition, survey results obtained from the university user community for one of the e-learning services were examined. Findings from the study were presented as user security requirements and recommendations, when planning future security initiatives of the e-learning services within the university.

Acknowledgements

First and foremost, I would like to thank my family, in particular my parents, William & Marie, and my sister Audrey. I am forever indebted to you for your endless support, understanding and eternal belief in my abilities.

In addition, I would like to thank my friends and colleagues for their encouragement, guidance and most importantly, for making me laugh when it was most needed! Finally, I would like to acknowledge and thank my advisor, Erik L Moore and the facilitators of the Masters in Software and Information Systems course, for gracing me with their support, time and expertise throughout the completion of my studies.

Table of Contents

Abstract	i
Acknowledgements	ii
Table of Contents	iii
List of Figures	v
List of Tables	vi
1 Chapter 1 – Introduction	7
1.1 Significance of the Study	7
1.2 Thesis Scope.....	2
1.3 Thesis Layout	2
2 Chapter 2 – Review of Literature and Research	3
2.1 Introduction	3
2.2 The Role of Authentication	5
2.3 Privacy Concerns.....	8
2.4 Types of Security Attack.....	14
2.5 E-learning Standards	18
2.6 E-learning Standard Organisations.....	22
2.7 Conclusion.....	25
3 Chapter 3 – Methodology	26
3.1 Introduction	26
3.2 Advantages & Disadvantages.....	27
3.3 Qualitative Research	27
3.4 Qualitative Research Methodology Designs	28
3.5 The Case Study Design	28
3.6 Conclusion.....	30
4 Chapter 4 –Analysis & Results	31
4.1 Comparative Analysis of the VLE Services.....	31
4.1.1 Architectural Comparison	31
4.1.2 Data Protection Policy Comparison.....	35
4.1.3 Comparative Analysis Conclusion.....	39
4.2 VLE Student User Survey	40
4.2.1 Survey Analysis and Result Structure.....	40
4.2.2 Survey Data Presentation:	41
4.3 User Survey Results	42
4.3.1 Demographic Profile.....	42
4.3.2 Demographic Summary:	48
4.4 VLE Usability	48
4.4.1 Barriers and Enablers	52
4.4.2 Survey Conclusion	63
5 Chapter 5 – Project History.....	65
5.1 Introduction	65
5.2 The Research Approach	65
5.3 Research Objectives	66

5.4	Conclusion.....	69
6	Chapter 6 – Conclusions	70
6.1	Introduction	70
6.2	Study Conclusion	70
6.3	Contribution	71
6.4	Lessons Learned	72
6.5	Future Research.....	72
	References	73
	Annotated Bibliography.....	85

List of Figures

Figure 1: Depicts learning standards and the relationships between them (Igras, 2003).....	21
Figure 2: Gender Results.....	42
Figure 3: Age Results.....	43
Figure 4: Field of Study Results.....	44
Figure 5: Student Type Results.....	45
Figure 6: Disability Assessment Results	46
Figure 7: Access by Location Results.....	46
Figure 8: Access by Time Results.....	47
Figure 9: Usage Frequency Results.....	48
Figure 10: Usage Benefit Results.....	49
Figure 11: Non-Usage Results.....	50
Figure 12: Subject Usage Results.....	51
Figure 13: Electronic File Sharing Results.....	53

List of Tables

Table 1: The Ten Privacy Principles used in Canada (El-Khatib et al, 2003).....	9
Table 2: Ten principles (Bevanda et al, 2009).....	11
Table 3: Attack Methods and Security Vulnerabilities (Stapić et al, 2008).....	14
Table 4: Course Notifications via Facebook Results.....	55
Table 5: Course Accessibility via iPhone/iTouch Results.....	55
Table 6: User Familiarity of Exam Functionality.....	57
Table 7: User Interest in using Exam Functionality.....	58
Table 8: User Familiarity of Assignment Submission Functionality.....	58
Table 9: User Interest in using Assignment Submission Functionality.....	59
Table 10: User Familiarity of Accessing Provisional Grades Online.....	60
Table 11: User Interest in Accessing Provisional Grades Online.....	60
Table 12: Registered Student Only Access Results.....	62
Table 13: All University Personnel Access Results.....	62
Table 14: Anyone/Anywhere Access Results.....	62

1 Chapter 1 – Introduction

As adoption of e-learning and lifelong learning grows, it is vital that the administrator of a virtual learning service ensures reliable and secure data. The nature of a virtual learning environment is not only to contain the student details but also the student's submitted work and their academic results, hence data protection is essential (Charlesworth, 2008). On implementing a virtual learning environment solution a University will strive to ensure the environments architecture and communication systems are robust and certainly secure from a physical and organizational stand point. However how many universities take the time to analyze the value of the data the virtual learning service holds and how it may be compromised?

1.1 Significance of the Study

Related research on the area of e-learning and security do discuss some of the issues which can be experienced when providing an e-learning service. Examples of such research would be, Borcea-Pfitzmann, Liesebach & Pfitzmann (2005) discussion on providing privacy for users while ensuring the environment is collaborative, Cárdenas & Sanchez (2005) presentation of the security challenges of distributed e-Learning, Gong, Qiang & Wang (2009) presentation of a security model which could aid online learning; or the security framework by Mwakalinga et al, (2009), which provides criteria to aid an e-learning system in adapting to environments and to the culture of e-learning users. However, by considering the existing research and Ingerman & Yang (2010, May/June) ranking of security at number three in the top ten IT issues of strategic importance to technology leaders in higher education. A study of e-learning services from a user community perspective within the realm of a university seemed to be required.

This study will take the first steps into analyzing the use and security needs of a virtual learning environment by performing a case study of a university in Ireland The thesis proposal is

to examine the existing data security features of the Virtual Learning Environments (VLE) of the Irish university, and assess how the security strengths of these systems could be combined with external security measures to provide greater data security for the university.

1.2 Thesis Scope

The scope of the thesis is to conduct a comparative analysis of the security features of the two main e-learning services in use by the university. Complete a survey of user feedback regarding security components of the existing e-learning services on campus, which will aid in determining the security requirements of the university and finally an analysis of available security technologies, which will lead to security recommendations for the university.

1.3 Thesis Layout

This introduction chapter is the first of six chapters contained in the thesis. In addition, an annotated bibliography is provided for all literature reviewed in the study. The chapter's divide the case study research as follows:

- Chapter 2 - provides a review of existing literature in the area of e-learning systems and security.
- Chapter 3 - outlines what methodology was used to complete the study and why it was chosen.
- Chapter 4 - provides the analysis and results of the comparative analysis of the e-learning services in use by the university and the results of the user survey.
- Chapter 5 - provides a review of how the research was conducted
- Chapter 6 - provides a summary of the case study findings, challenges encountered and suggestions regarding areas of future research.

2 Chapter 2 – Review of Literature and Research

The following chapter provides a review of existing literature in the area of e-learning systems and security.

2.1 Introduction

Lifelong learning is becoming a necessity for the continued success of an individual and in fact for the continued success of the company (Graf, 2002). For this to be achievable; new knowledge must be transferred in a seamless manner while also having a minimum impact on both the working and personal lives of an individual, (Graf, 2002).

Welcome the era of e-learning. The advancements made in technology has progressed teaching to a new realm, a way of supporting learning throughout the world (Tsiantis, Stergiou & Margariti, 2007). E-Learning offers the advantages of enabling users to learn any time, in any location, independently or assisted (Borcea, Donker, Franz, Pfitzmann & Wahrig, 2006). Igras (2003) states that e-learning systems can be a simple system which helps the author create a web page with text, some graphics, and possibly a video clip. This type of system allows the user to choose the courses they are interested in, and basically read a book in electronic form or a complex system which maintains a user's credentials and preferences, prescribe appropriate courses from available options, monitor and evaluate progress through the course, and award the user credit based on an assessment test. This type of system can also provide an environment to integrate learning-related activities, such as access to e-mail, virtual classrooms, etc. For the purpose of this thesis the term e-learning will be used to reference the latter.

One of the first e-learning systems was called Plato. This system was developed by the university of Illinois in 1960 and was finally decommissioned in 2006 (Stapić, Orehovački, & Danić, 2008). This system pioneered key concepts such as online forums, online testing, chat

rooms, and remote screen sharing. Following the development of Plato, a flood of similar systems were introduced, however in this study only a few of the main vendors will be mentioned. In 1997, WebCT 1.0 was released and Blackboard was founded. The introduction of Moodle followed in 1998 and was fully launched by 2001 (Stapić, Orehovački, & Danić, 2008). Although today there may be greater than 150 different systems providing e-learning services, it is the design and functionality of these services which needs to be carefully considered (Stapić, Orehovački, & Danić, 2008). Eibl (2008) states that in the theory of constructivism, learning is no longer considered as externally transfusing knowledge. Learning is considered as an active process of constructing knowledge. Therefore the activity and participation in the learning process need to be transferable to informatics systems. Borcea-Pfitzmann, Liesebach & Pfitzmann (2005) propose that to design an e-learning environment, two main principles should be considered, (1) The behaviour of the e-learning users behaviour within the electronic environment ideally should correspond closely to the users natural behaviour in the real world, and (2) Each user should have free access to all functionalities offered by the environment within the frame of agreed rules and directives

Current e-learning systems are complex applications, which allow users to participate in a wide variety of tasks related to learning and provide a supported cooperative learning environment (Borcea et al, 2006). However with this ability comes the responsibility of security. Cárdenas & Sanchez (2005) state that e-learning trends demand a high degree of interoperability for applications, learning systems and heterogeneous system; this has created the knock on affect of increasing the challenges of security issues. Confidence in a systems ability to reliably protect data is of utmost importance to ensure users trust in the online learning environment. However some implementations of security mechanisms can have a negative

impact on the usability of the environment. Tsiantis, Stergiou & Margariti, (2007) states the two main security issues which present usability issues are authentication and privacy. So for e-learning to truly succeed, Tsiantis, Stergiou & Margariti, (2007) suggest that security mechanisms implemented to protect user's data must be implemented according to the user's needs.

So to fully grasp the importance of a discussion on the role of security in an e-learning environment it is important to define the general role each endeavour to play. Tsiantis, Stergiou & Margariti (2007) provide the following explanation for each:

“A true learning environment thrives upon a tradition which provides an area of trust, information exchange and discussions. While within a security domain the opposite is true, this domain relies on a culture of distrust, restricted information flow and autocratic rules”

For this study, the statement of security needs to be narrowed to specifically the area of computer security. In general this type of security relates to malicious or accidental behaviour and therefore focuses more on human behaviour rather than a computer malfunction (Tsiantis et al, 2007).

2.2 The Role of Authentication

One method used to increase the security of an e-learning environment is authentication.

The process of authentication contains two main stages, they are:

- (1) User Identification - usually achieved by an allocated id which does not require securing
- (2) User Verification – proof the user is the owner of the id, which is secure.

Tsiantis, Stergiou & Margariti (2007) reference three ways in which a user may authenticate to an e-learning system, (1) Knowledge-based authentication, a user provides information to the system which only the user would know, (2) Token-based authentication, the user provides the

system with something only they possess and (3) Biometrics, the computer measures something specific to the users person. Currently Knowledge-based authentication is the most common method of authentication primarily due to its simplicity. However, although Knowledge-based authentication has a “universal appeal”, it does have the disadvantage of poor usability (Tsiantis et al, 2007). Passwords and pins which are popular knowledge based authentication mechanisms rely on the user’s ability to recall correct data.

Additionally as technology becomes more and more involved in people’s lives, the number of pins and passwords required can become excessive. Online learning programs are not the exception, they also demands the use of password-authentication rather than other ways of authentication. This results in a possible challenge for users, with the number of items to recall and the added complexity of the data to remember (Tsiantis et al, 2007). However Eibl (2008) states that “to truly allow a system to vanish behind learning objectives, system-related user interaction should be minimized. For example, if there are several systems put together with authorization requirements in each of them, single sign-on solutions like Shibboleth, Kerberos, or the Lightweight Directory Access Protocol (LDAP) are sensible”. With regard to how often a password should be changed is purely dependent on the level of confidential data being held. Tsiantis et al. (2007) state that the “change regime of a password does not increase security but does decrease the level of damage should a breach occur”.

A method proposed by Kambourakis, Kontoni, Rouskas & Gritzalis (2004) describes how public key certificates and attribute certificates, organized under a Public Key Infrastructure, could provide strong authentication and fine-grained trust control of common e-learning services. As users and providers rush to adopt e-learning, they become aware of the need for security features and protection of their privacy. And as such put a demand on more

flexible, dynamic and scalable mechanisms which are necessary to support anytime/anywhere services and solutions in a many-to-many trust model integrated with the unsecured Internet environment (Kambourakis et al, 2004). In the context of e-learning, attribute certificates can be effectively implemented by deploying primary key technology and RBAC logic to these systems which in turn will provide authentication, authorization, tamperproof evaluation of tests and protection of courseware material. This method will provide mutual trust for both the learners and service providers (Kambourakis et al, 2004).

Although the need for authentication cannot be dismissed, Graf (2002) presents a view that regardless of the authentication method used, a conceptual problem will still exist. That is although the authentication may ensure a certain user has been involved in a certain learning activity, it cannot guarantee the users actions recorded are original to the user and not in fact obtained via an illegitimate resource. To achieve absolute security is not possible, even if teaching was to return to the traditional methods of classroom controlled environments (Graf, 2002). This method too had to allow users to work away from the controlled environment in order to achieve the teaching requirements, i.e. assignments separate to the teaching. So to that end absolute security cannot be achieved however the primary goal for e-learning should be to achieve an adequate amount of security as that established for the traditional methods (Graf, 2002). The following are some of the methods suggested to achieve this:

- (1) Legal steps: - a user is required to sign a legal document stating no use of illegitimate resources, (Graf, 2002),
- (2) Separations of learning and certification – allow the user to learn online but be examined in a controlled environment. This approach provides a high level of security but is in fact

removing some of the main reasons for the development of e-learning, i.e. to gain knowledge independent of time and location, (Borcea et al, 2006).

(3) Integrated testing – this is continuous assessment based on the users overall involvement in the online learning experience, i.e. completion of tasks from discussions boards, assignments, etc (Graf, 2002),

(4) Innovative course design – this method would be a large overhead for the course instructor as it involves the development of a course which requests the user accomplish a task based solely on the knowledge they have gained, i.e. open book exams. This method ensures the user has a complete understanding of the knowledge area (Graf, 2002).

2.3 Privacy Concerns

Jerman-Blazic & Klobucar (2005) state that Privacy is understood as a freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual. Research in the complex application area of e-learning mainly focuses on topics directly related to learning (Borcea et al, 2006). However many articles stress the additional importance of considering privacy topics. Borcea et al. (2006) go to explain that every action within a computer-based system implies the accrue of data. This automatically creates a trace of the user's actions while traversing the system which by default will be picked up on by monitoring. This data can be gathered to create a fairly detailed profile of the users and by association can increase privacy threats.

In relation to security, the ownership of data can also be defined as the user's access and manipulation rights of the data. In this context, the ownership can then map to confidentiality and integrity, (Tsiantis et al, 2007). To take this point further, Tsiantis et al. (2007) explore the possibility that it is actually the user's concept of ownership that is intertwined with privacy and

to understand the privacy levels required, it is important to first understand the user's perception of data ownership and privacy. This will ensure the correct understanding of what needs to be protected and how it should be protected will be ascertained, (Tsiantis et al, 2007). As Borcea et al. (2006) succinctly put it, "users must be able to control which information others know about them. Appropriate use of technologies can provide privacy and data protection. However, these technologies do require relevant attributes in the databases which not obvious in the existing e-learning standard schemes (Jerman-Blazic & Klobucar, 2005). This raises a valid point, how does one know if relevant attributes are set or for that matter if the application has the ability to meet privacy requirements. Both El-Khatib, Korba, Xu & Yee (2003) and Bevanda, Azemović & Mušić (2009) reference the ten privacy principles in an attempt to provide frameworks which will evaluate and possibly improve the privacy abilities of e-learning systems.

El-Khatib et al. (2003) suggest an applications ability to meet privacy requirements should be assessed and provide a table which describes the ten Privacy Principles incorporated in the Personal Information Protection and Electronic Documents Act of Canada. While the outlined principles in Table 1: The ten Privacy Principles used in Canada (El-Khatib et al, 2003) can be challenging to realize in any sector, they do offer a means for critiquing the appropriateness of different technologies. Note each principle may be implemented in computer systems to varying degrees due to the nature of each principle.

Table 1: The Ten Privacy Principles used in Canada (El-Khatib et al, 2003).

<i>Principle</i>	<i>Description</i>
Accountability	An organization is responsible for personal information under its control and shall designate an individual or individuals accountable for the organization's compliance with the privacy principles.

Identifying Purposes	The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
Consent	The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.
Limiting Collection	The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
Limiting Use, Disclosure, and Retention	Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. In addition, personal information shall be retained only as long as necessary for fulfilment of those purposes.
Accuracy	Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
Safeguards	Security safeguards appropriate to the sensitivity of the information shall be used to protect personal information.
Openness	An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
Individual Access	Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to

	that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
Challenging Compliance	An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

However Bevanda et al. (2009) proposed the application of the Hippocratic database concept on the databases of e-learning systems in an effort to prevent unauthorised access to shared resources. The Hippocratic database concept is based on the principles of the Hippocratic Oath, in order to provide data privacy and confidentiality. To this end, Bevanda et al. (2009) stated that if used and implemented correctly the principles in Table 2: Ten principles (Bevanda et al, 2009) should guarantee privacy of data.

Table 2: Ten principles (Bevanda et al, 2009)

1	Purpose specification. For personal information stored in the database, the purposes for which the information has been collected shall be associated with that information.
2	Consent. The purposes associated with personal information shall have consent of the donor of the personal information.
3	Limited collection. The personal information collected shall be limited to the minimum necessary for accomplishing the specified purposes.
4	Limited use. The database shall run only those queries that are consistent with the purposes for which the information has been collected.
5	Limited disclosure. The personal information stored in the database shall not be communicated outside the database for purposes other than those for which there is

consent from the donor of the information.

- 6 Limited retention. Personal information shall be retained only as long as necessary for the fulfilment of the purposes for which it has been collected.
 - 7 Accuracy. Personal information stored in the database shall be accurate and up-to-date.
 - 8 Safety. Personal information shall be protected by security safeguards against theft and other misappropriations.
 - 9 Openness. A donor shall be able to access all information about the donor stored in the database.
 - 10 Compliance. A donor shall be able to verify compliance with the above principles. Similarly, the database shall be able to address a challenge concerning compliance. For now there is no technical or commercial implementation of this or similar principles of hDB.
-

Bevanda et al. (2009) believe that in the case of eLearning environment implementing the principles of Hippocratic Databases could prevent privacy violation which can involve students, educational and administration staff. The application of the principles could also simplify access control policy administration tasks. However unfortunately current trends and solutions tend to put privacy issues low on the priority list and expect a company's security policy to handle them. Ideally access control and security mechanisms should just be part of the technology to ensure data privacy of the data (Bevanda et al, 2009).

Eibl, von Solms & Schubert (2006) also developed a framework for evaluating the security capabilities of an e-learning system. The framework contains a criteria catalogue, which can be used to check whether the security concept of an e-learning platform is sufficient to be

used in a productive environment. Eibl et al. (2006) based the criteria catalogue on the following six information security services which need to be in place to create a secure environment.

- a. Confidentiality - to ensure that data stored in databases and transmitted over a network, cannot be read by unauthorized third parties,
- b. Integrity - to ensure that data stored in databases and transmitted over a network cannot be changed by unauthorized third parties,
- c. Availability - to ensure that data is available to authorized parties at all times,
- d. Identification and authentication - to ensure that a learner is properly identified and verified during the log-on process,
- e. Authorization - to ensure that the user only has access to that data which is relevant to him/her, and not to other data, and
- f. Non-repudiation - to ensure that a user can be held individually responsible for any action performed on the system.

By aligning the criteria against these services, Eibl et al (2006) ensured the catalogue was following an internationally accepted model for information security in ICT systems.

Unfortunately this framework only considers the security concept and not the quality of the implementation.

Regardless of the method used to mitigate the privacy risks, it is important to note that users cannot act completely anonymously in an eLearning system. Collecting and evaluating personal information is a necessary evil if basic tasks such as providing assistance for users or realizing assessments, are to be performed. A total solution for privacy provision cannot be therefore based on technology only; it must combine laws, markets and technology (Franz & Borcea-Pfitzmann, 2006; Jerman-Blazic & Klobucar, 2005).

2.4 Types of Security Attack

Gong, Qiang & Wang (2009) explain how enterprises established information interaction platforms through internet, in order to manage information in a rapid and efficient way; unfortunately, due to vulnerabilities these enterprise information systems including the internet are under malicious attacks which can cause damage to an organizations reputation. Therefore the discussion of security issues needs to be broader than just authentication and privacy, it also needs to include how an attack can occur, the type of attack and the various system layers it may affect, (Cárdenas & Sanchez, 2005).

Stapić, Orehovački, & Danić (2008), provide table 3: Attack methods and Security Vulnerabilities (Stapić et al, 2008) which displays a summary of classified attack methods and vulnerabilities independent of the specific e-learning implementation.

Table 3: Attack Methods and Security Vulnerabilities (Stapić et al, 2008).

Authentication attacks (the identity & password of a legitimate user is stolen by an attacker steals, with the goal of free access to paid e-learning services.)

- (1) Broken authentication and session management, vulnerability which occurs because account credential management functions and session tokens are not often properly protected.
- (2) Insecure communication, vulnerability which appears during transmits of sensitive information without proper encryption.

Availability attacks (The attack goal is to ensure e-learning services and data are unavailable to authorized end-users)

- (1) Denial of service – is one of the most popular forms of availability attack. The aim of this type of attack is to misuse finite bandwidth and connectivity resources of LMS system
-

Confidentiality attacks (The attack goal is not data modification but data access and dissemination.)

- (1) Insecure cryptographic storage, e-learning systems rarely uses cryptographic functions properly to protect data and credentials or may use weak encryption algorithms. This allows for valuable data to be relatively easy to access, e.g. an attacker using identity theft.
- (2) Insecure direct object reference can occur when an e-learning system uses object references directly in web interfaces without authorization checks being implemented.
- (3) Information leakage and improper error handling, e-learning systems can leak sensitive information about its logic, configuration and error messages generated can display too much information, which proves useful in the hands of an attacker.

Integrity attacks (attempt to create new data or modify and even delete existing e-learning data)

- (1) Buffer overflow - occurs when an e-learning component tries to store data into an available buffer without validating its size. This can enable malicious code to be executed.
 - (2) Cross Site Request Forgery, client side attack which exploits trust that an e-learning system has for a user
 - (3) Cross Site Scripting, is a hacking technique which allows an attacker to supply vulnerable dynamic web page with malicious script and execute script in victim's browser in order to gather data from a user.
 - (4) Injection flaws, occurs when data provided by user is sent to content checking routines as part of a command or query
 - (5) Failures to restrict URL access, some e-learning resources are restricted to a small subset
-

of privileged users. This weakness allows an attacker to retrieve URLs by guessing the address and perform unauthorized operations on unprotected data.

- (6) Malicious file execution, attack based on the fact that e-learning systems fail to control/prohibit execution of uploaded files
-

The majority of the vulnerabilities highlighted in the table above depend on the system architecture as much as the implementation and server settings of the system (Stapić et al, 2008). For example, at the application level, an attack can result in one or more requests being blocked indefinitely, at the network level, a symptom of an attack can be abnormal traffic volume in a network segment and at the operating system level, some attacks will display symptoms of unusual programs or scripts, or unusual CPU load, (Cárdenas & Sanchez, 2005).

This point is further emphasised by Gong et al. (2009) who states that even though enterprises that are connected through the internet, share basically the same operating system, communication protocols and databases, enterprises can vary in numerous ways from type, complexity, degree of information and property values of information. Thus, we need to deploy security measures of different levels, so as to minimize expected security loss. Mwakalinga, Kowalski & Yngström (2009) developed a security framework that considers culture of users and environments where information systems operate. The security framework is based on the Systemic-Holistic approach and the principles of the immune system. This framework contains components such as: the management system, the adaptability system, the deterrence sub system, the prevention sub system, the detection sub system, the response sub system, and the recovery sub system. The security framework provides measures that help an e-learning system learn to adapt to environments and to culture of e-learning users. (Mwakalinga et al, 2009).

In order to determine the optimal security settings for an e-learning environment all software and hardware configurations need to be considered as each factor will impact the security design, this includes all elements across the internet and intranets, (Stapić et al, 2008; Cárdenas & Sanchez, 2005). Franz & Borcea-Pfitzmann (2006) propose a method which involves partitioning personnel data within the e-learning application. This method stems from a known approach to preserve privacy despite the need for collecting and processing personal data by partitioning the data by means of Privacy-Enhanced Identity Management (PIM). Users are enabled to decide on their own which data is delivered to whom after considering the current situation (Franz & Borcea-Pfitzmann, 2006).

The method of partitioning is usually considered between different applications or service providers. However Franz & Borcea-Pfitzmann, (2006) considered the fact that an e-learning application actively creates numerous scenarios which involve cooperation between users and as such would it not be worth considering partitioning within the application. Intra-application partitioning would allow a user to act under different partial identities within one application (Franz & Borcea-Pfitzmann, 2006). To achieve this Franz & Borcea-Pfitzmann (2006) made two assumptions:

- The functionality for generating and managing partial identities would be provided by a PIM system.
- The application would have the ability to define which events could imply a switch to another partial identity.

This introduction of intra-application partitioning would aim at maintaining a user's privacy and ultimately prevent linking between all actions of a user, thus allowing the user to work unrestricted in an unbiased environment (Franz & Borcea-Pfitzmann, 2006).

The benefits of providing learning systems on the internet cannot be denied. They allow for unlimited opportunities with regard to reducing costs and increasing efficiency, (Cárdenas & Sanchez, 2005). Ultimately though with every benefit comes a negative, the fact the internet provides greater access to data is of course of great interest to the genuine users however this data can be of even greater interest to a hacker, (Cárdenas & Sanchez, 2005). As Tsiantis et al. (2007) suggest, the future of security design for online learning software lies ideally, with the collaboration between users and experts to develop the usable mechanisms required.

2.5 E-learning Standards

Standards can be defined as documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics, to ensure that materials, products, and services are fit for their purpose and as it is universally accepted that e-Learning is the best vehicle for supplementing the knowledge beyond the classroom, the design and development of standards needs to be put in place to ensure consistency and transferability of skills. (Jerman-Blazic & Klobucar, 2005; Babu, 2001). The good news is that e-learning has finally shifted from a chaotic “no standards” stage, to a phase of rules and standards definition (Varlamis & Apostolakis, 2006).

In the context of e-learning, technology standards are generally developed to be used in the system design and implementation for the purposes of ensuring interoperability, portability and reusability (Jerman-Blazic & Klobucar, 2005). Standards impose a certain order by providing more uniform and precise access and manipulation to e-Learning resources and data (Babu, 2001). Thus ensuring the learning content is both interoperable with learning management systems and easily re-useable by other developers across participating organizations (Igras, 2003). There are number of organizations (e.g. IMS, ADL, ARIADNE, IEEE, ISO) working to

develop specifications and standards (Babu, 2001). The dominance of platform independent, open technologies and promote user-centric e-learning systems will be facilitated by the adoption of standards and specifications (Varlamis & Apostolakis, 2006).

Unfortunately almost all e-learning standards appear to be focusing on e-learning system design, course development and delivery, system interoperability and scalability; with little focus spent on possible security concerns (Yong, 2007). However while more e-learning systems are formally used by educational institutions and even more e-learning systems adopt open source technology, the e-learning security concerns will become inevitable (Yong, 2007). Babu, (2001) outlines some benefits which can be expected if appropriate standards are available, they are:

- Industry-wide standards for learning technology systems architectures.
- Common, interoperable tools used for developing learning systems.
- A rich, searchable library of interoperable, plug-compatible learning content.
- Common methods for locating, accessing and retrieving learning content.
- Standardized, portable learner histories that can be transferred with the learner over time.

Varlamis & Apostolakis, (2006) also provide a list of merits based on the use of standardised technologies, which would protect e-learning investments, they are:

- Interoperability - Content from multiple providers can be easily disseminated within consumers and a multitude of systems.
- Re-usability - Content and code can be assembled, disassembled, and re-used quickly and easily.
- Manageability - Systems can track the appropriate information about the learner and the content.

- Accessibility - A learner can access the appropriate content at the appropriate time on the appropriate device.
- Durability - Content is produced once and transplanted many times in different platforms and systems with minimum effort.
- Scalability - Learning technologies can be expanded in functionality in order to serve broader populations and organizational purposes.

Unfortunately a difficulty with e-learning standards is that although products may claim to conform, they do not actually work together without further configuration (Varlamis & Apostolakis, 2006). However Jerman-Blazic & Klobucar, (2005) state the outcome of the standardization efforts can be divided into two levels

(1) Specification of the information models involved.

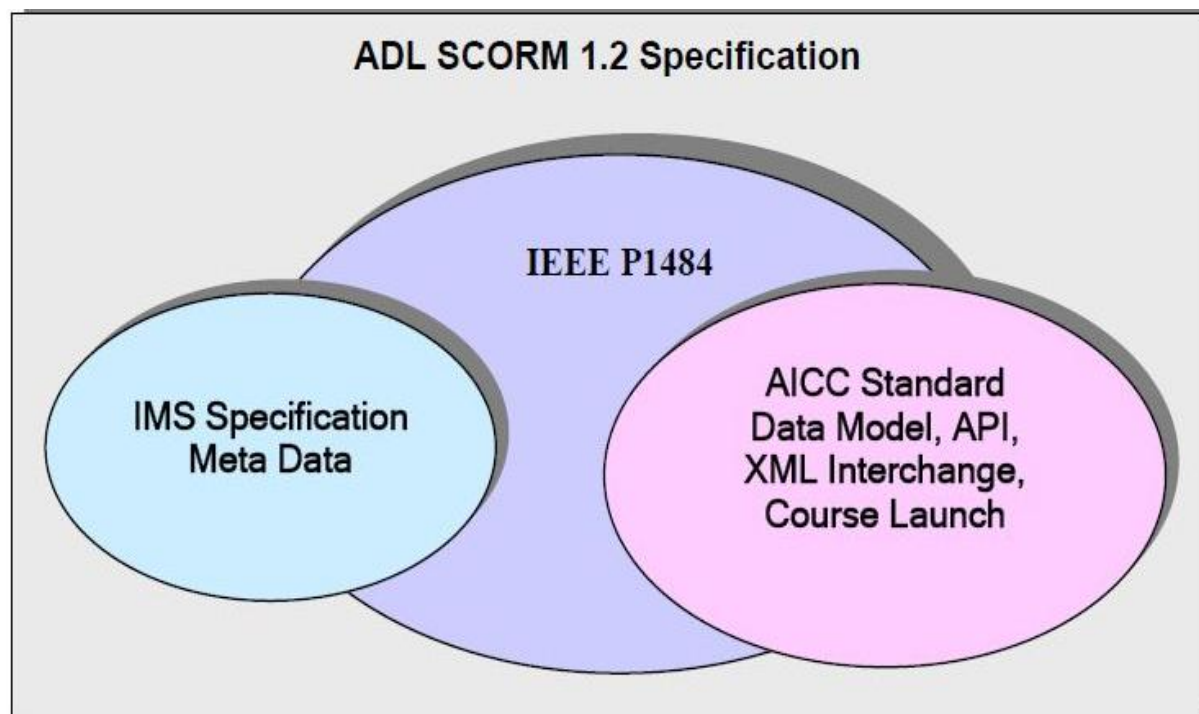
(2) Specifications of the architectures, software components and provided interfaces.

The more mature results regarding e-learning standardization correspond to the first level (Jerman-Blazic & Klobucar, 2005). At the second level, e-learning standards define the expected behaviour of software components responsible for managing learning objects in online environments Jerman-Blazic & Klobucar, 2005).

Nonetheless, to ensure the success of setting standards, it is necessary that e-learning standards must be adopted by everyone without any customization or modification (Varlamis & Apostolakis, 2006). The standards evolution initially began in 1994 with the Dublin Core Meta data framework for web resources, following this in 1997 the IMS (Educause consortium), open market based standards for online learning was created and the NIST & IEEE P1484 merged with IMS effort to begin a collaboration with ARIADINE (Babu,2001). Finally in 1998,

IME in collaboration with ARIADINE submitted a proposal and specification to IEEE which formed the basis for the current IEEE Learning Object Meta data base document (Babu, 2001). Over the past number of years, groups have continued to actively work on developing industry wide standards for e-learning. These groups include organisations such as: Aviation Industry CBT [Computer-Based Training] Committee (AICC), IEEE Learning Technology standards Committee, IMS Globe Consortium, Advanced Distributed Learning- Sharable Content Object Reference Model (ADL-SCORM) and Alliance of Remote Instructional Authoring and Distribution Networks for Europe (ARIADNE (El-Khatib et al, 2003 & Yong, 2007)). The focus for the majority of these groups is content management, meta-data specification, or other areas with little reference to security and privacy (El-Khatib et al, 2003).

Figure 1: Depicts learning standards and the relationships between them (Igras, 2003).



2.6 E-learning Standard Organisations

AICC – is an international group of technology-based training professionals that creates CBT-related guidelines for the aviation industry (Yong, 2007). The AICC specifications define how content units (learning objects) communicate with Learning Content Repositories and Learning Management Systems (www.aaic.org), (Igras, 2003). The organisation is mainly known for the (1) creation of well developed specifications for learning, (2) a focus on reuse and interoperability of online learning and (3) coordinating efforts with broader learning technology standards, i.e. LTSA of IEEE and ADL.

ARIADINE – is focused on the development of tools and methodologies for producing, managing and reusing computer based pedagogical elements. They are involved in related technical specification efforts in the area of meta-data and in collaboration with IMS jointly developed a meta-data specification for submission to IEEE, (Babu, 2001).

ADL – is a U.S. government-sponsored organization that researches and develops specifications to encourage adoption and advancement of e-learning. The most widely accepted ADL publication is the ADL Shareable Content Object Reference Model (SCORM), which combines the best elements of IEEE, AICC, and IMS specifications into a consolidated document (Yong, 2007). ADL is known for developing guidelines needed for large scale development and implementation of efficient and effective distributed learning and for providing a forum which allows for requirements input into the IMS specification process, (Babu, 2001). SCORM is an example of the application and integration of the learning standards and consists of three main sections: an Extensible Mark-up Language (XML)-based specification for representing course structures; a set of specifications relating to the run-time environment, including an API, content-to-LMS data model, and a content launch specification; and a

specification for creating meta-data records for courses, content, and raw media elements (www.adlnet.org) (Babu, 2001; Igras, 2003).

IMS (Instructional Management System) Global Learning Consortium was founded in 1997, and originally focused on higher education. The IMS project now focuses on a range of initiatives relating to standards for learning servers, learning content and the enterprise integration of these capabilities (Babu, 2001). The IMS consortium has members from educational, commercial, and government organizations (Babu, 2001).

Babu (2001) states that the Key goals of IMS consortium are:

- Defining the technical standards for interoperability of applications and services in distributed learning
- Supporting the incorporation of IMS specifications into products and services
- Widespread adoption of specifications that will allow distributed learning environments and content from multiple authors to work together

El-Khatib et al. (2003) and Babu (2001) highlight the series of reference specification provided by IMS to address key problems and challenges in distributed learning environments, they are:

(1) Meta-data Specifications - Meta-data are attributes in the form of XML (eXtensible Mark-up Language) tags attached to e-learning resources, (2) Enterprise Specification - establishes formats for exchanging student and course information between system components, i.e. between the e-learning systems and possibly a student information system, (3) Content & Packaging Specification - provides instructions for wrapping and exchanging learning content. This helps port learning content from one e-learning system to another, (4) Question & Test Specification - specification establishes formats for constructing and exchanging assessment information, (5) Simple Sequencing Specification, and (6) Learner Information Package Specification.

In particular the IMS Learner Information Package (IMS LIP) Specification addresses the interoperability of learner information systems with other systems that support the Internet learning environment. The IMS LIP treats data privacy and integrity as essential requirements but unfortunately does not define any details of implementation mechanisms or architectures that could be employed to support privacy protection (El-Khatib et al, 2003).

IEEE is an international organization that develops technical standards and recommendations for electrical, electronic, computer and communication systems (Yong, 2007). Within the IEEE, the Learning Technology Standards Committee (LTSC) provides specifications that address best practices (Yong, 2007). The LTSC has over a dozen working groups and study groups developing accredited standards for learning technology, (Babu, 2001). The most widely acknowledged IEEE LTSC specification is the Learning Object Metadata (LOM) specification, which defines element groups and elements that describe learning resources (Yong, 2007). The IEEE P1484 is a standard for learning technology proposed by the Learning Technology Standards Committee (LTSC) of the IEEE Computer Society (El-Khatib et al, 2003). The specification of Public and Private Information (PAPI) for Learners (P1484.2) outlines the syntax and semantics as well as the privacy and security of learner's information (El-Khatib et al, 2003). The standard permits different views of the learner information and substantially addresses issues of privacy and security (Jerman-Blazic & Klobucar, 2005). It categorizes the security and privacy concerns from the point of view of different stakeholders, such as developer, institution, regulator, and user (El-Khatib et al, 2003).

Two parts of the PAPI Learner standard are directly related to security and privacy issues. IEEE 1484.2.3 gives information and recommendations on important security issues for implementations, while 1484.2.23 describes learner security information, e.g., keys and

credentials (Jerman-Blazic & Klobucar, 2005). As for privacy concerns, the P1484.2 does not specify a detailed model or technologies. It states that the implemented security techniques, including physical security, confidentiality, etc. can all be used to provide privacy (El-Khatib et al, 2003). The PAPI standard introduces by definition notions that are relevant for provision of security and data protection by specifying the meaning of terms related to access control, administrative security, authentication, authentication exchange, integrity (data) authentication information, computer security, confidentiality, learner credentials, inbound security threat and digital signature (Jerman-Blazic & Klobucar, 2005).

Another of the IEEE specifications is the IEEE LTSA which specifies a high level architecture for information technology-supported learning, education, and training systems, (Igras, 2003). The IEEE LTSA specification corresponds to a conceptual model applicable to a broad range of learning scenarios and consists of a number of layers (Jerman-Blazic & Klobucar, 2005; Babu, 2001).

2.7 Conclusion

The literature review provided a valuable insight into the world of e-learning and the discussion of possible security and privacy concerns. The papers reviewed spanned from 2001 to 2009, showing the topic of e-learning security to really only be in its infancy. Although each paper has provided thought provoking discussion, none provided a concise security requirements guide for online learning activities which could be applied to a university managed e-learning environment.

3 Chapter 3 – Methodology

There are two main research methodologies to choose from when embarking on a research project. They are Qualitative and Quantitative research methodologies. For the purpose of this study the Qualitative research methodology was selected. The following chapter outlines what this methodology entails and why it was chosen for this study.

3.1 Introduction

“To answer some research questions we cannot skim across the surface. We must dig deep to get a complete understanding of the phenomenon we are studying” (Leedy & Ormrod, 2005, p.133). Qualitative Research is one method used extensively by researchers to dig deep. The term encompasses investigative methodologies described as ethnographic, naturalistic, anthropological, participant observer, or field research, (Key, 1997). If minimum information is available on a topic or some variables are still unknown a qualitative study can help in determining what is important or in fact what should be studied (Leedy & Ormrod, 2005). As such a qualitative research approach tends to always have two main goals, (1) a focus on the phenomenon in its natural setting and (2) a study of the phenomenon in its complexity, (Leedy & Ormrod, 2005).

As Qualitative research is used to generate possible leads which can then be used to formulate a testable hypothesis, it is often regarded as a precursor to quantitative research. The testable hypothesis can be further tested and mathematically analyzed, using standard quantitative research methods, (Shuttleworth, 2008). This method of study however is not considered new by any means in fact many consider it to be one of the oldest of all scientific techniques, (Shuttleworth, 2008). An example of such being the Ancient Greek philosophers

qualitatively observing the world around them and attempting to develop a hypothesis on what they saw (Shuttleworth, 2008).

3.2 Advantages & Disadvantages

Some advantages of using Qualitative techniques is that

- (1) They are extremely useful when a subject is too complex to be answered by a simple yes or no hypothesis, (Shuttleworth, 2008).
- (2) They produce more in-depth, comprehensive information, (Key, 1997).
- (3) The techniques seek a wide understanding of the entire situation (Key, 1997).

However some of the disadvantages of using the qualitative techniques include:

- (1) they require a lot of careful thought and planning, to ensure that the results obtained are as accurate as possible, although the level of thought and planning is not to the same extent as the time/resource levels required to perform quantitative experiments, (Shuttleworth, 2008).
- (2) Qualitative data cannot be mathematically analyzed in the same comprehensive way as quantitative results, so can only give a guide to general trends. (Shuttleworth, 2008).

3.3 Qualitative Research

Leedy and Ormrod (2005) provide four examples of when to use a qualitative research study, they are: (1) Description: when the goal is to try and seek an understanding of the nature of a situation, process, system, people, etc. (2) Interpretation: the researcher wishes to produce theories, hypothesis based on data collected and gain new insight into the phenomenon, (3) Verification: the researcher would like to test these theories/assumption and finally (4) Evaluation: the researcher wishes to assess the effectiveness of a new procedure/policy, etc. Certainly the goal of this study was to improve the researchers understanding of security requirements for virtual learning environments and if possible produce a theory on the

requirements, based on data collected. From this point of view it made sense to use a qualitative research approach.

3.4 Qualitative Research Methodology Designs

The following outlines the five main types of Qualitative Research:

- (1) Grounded theory: uses a prescribed set of procedures for analysing data and constructing a theoretical model from them, (Leedy & Ormrod, 2005).
- (2) Phenomenology: Describes the structures of experience as they present themselves to consciousness, without recourse to theory, or assumptions from other disciplines. (Shuttleworth, 2008).
- (3) Ethnography: Focuses on the sociology of meaning through close field observation of the phenomena. (Shuttleworth, 2008). Typically, the researcher takes an in-depth look at a common culture (Leedy & Ormrod, 2005).
- (4) Content Analysis/Historical: Systematic examination and objective evaluation of data related to past occurrences in order to identify patterns, themes or biases, (Shuttleworth, 2008).
- (5) Case study: A particular individual, event, program is studied in depth for a specified period of time (Leedy & Ormrod, 2005).

3.5 The Case Study Design

For the purpose of this study the Case Study Qualitative research design was chosen. Case studies are detailed investigations of individuals, institutions or other social units (Key, 1997). The principle difference between case studies and other research studies is that the focus of attention is on the individual case and not the whole population of cases (Key, 1997). Although all methods do require a review of literature, a defined research question and analytic strategies using formal data collection protocols, and the ability to write a good research report; Case

studies require one additional skill, the ability to complete data collection and data analysis together (Yin, 2004). The complexity of case studies is generally due to the involvement of multiple sources of data, possible inclusion of multiple cases within a study, and the potential to produce large amounts of data for analysis (Soy, 1996). There are six main steps when performing a case study, they are:

1. Determine and define the research questions :

The first step in case study research is to establish a firm research focus to which the researcher can refer over the course of study of a complex phenomenon or object, (Soy, 1996). This was achieved in this thesis through the development of the thesis initial proposal and subsequently strengthened by the completion of a literature review.

2. Select the cases and determine data gathering and analysis techniques

During the design phase of case study research, the researcher determines what approaches to use in selecting single or multiple real-life cases to examine in depth and which instruments and data gathering approaches to use (Soy, 1996). Examples of the tools used to collect data are surveys, interviews, documentation review, observation (Soy, 1996). For the purpose of this thesis, the tools selected are that of a survey of the student VLE users and questionnaires for the system administrators of the two VLE systems.

3. Prepare to collect the data

Because case study research can generate a large amount of data it is important to have a systematic method of organising the data (Soy, 1996). This will ensure the researcher continues to keep sight of the original goal of the research and prevents the researcher from becoming weighed down with the amount of data (Soy, 1996).

4. Collect data in the field

Is completed by the researchers carefully observing the object of the case study and identify causal factors associated (Soy, 1996). This can also involve renegotiation of arrangements with the objects of the study such as the subtraction/addition of questions to interviews, etc, (Soy, 1996). It is important to note that case study research needs to be flexible, but when changes are made, they should be documented systematically (Soy, 1996).

5. Evaluate and analyze the data

The researcher will examine the collected raw data in a bid to draw interpretations between the research objective and the data collected (Soy, 1996). The analysis of the information gathered for this study includes organization and categorization of the survey data, interpretation and identification of the survey and questionnaire data gathered resulting in the production of the VLE security requirements for an Irish university.

6. Prepare the report

Case studies should report on the collected data in a way that transforms a complex issue into one that can be easily understood by the reader, (Soy, 1996). By doing this it will allow the reader to question and examine the study and reach an understanding independent of the researcher (Soy, 1996).

3.6 Conclusion

This chapter explained the purpose of using a methodology when completing a study and specifically the method used for this study. It outlined the steps involved in performing a case study and how this correlates with the objectives of this researcher's particular thesis.

4 Chapter 4 –Analysis & Results

This chapter provides the analysis and results of the two objectives of the study. First the comparative analysis of the VLE services in use by the university is presented, followed by the data results of a VLE user's survey, regarding online learning security and privacy.

4.1 Comparative Analysis of the VLE Services

The comparative analysis is divided into two sections: The first focused on comparing the VLE service architectural designs, while also taking into consideration the Irish data commissioner guidelines of issues which should be considered when developing security policies. The second focused on the primary VLE service policy and procedures as compared against the Irish data protection policy, while also taking into consideration the software vendor guidelines of privacy in relation to the application.

4.1.1 Architectural Comparison

The two e-learning services in use by the university are:

- A service used by all staff and students, which utilises the Blackboard Learning System software. The vendor of this software, Blackboard Inc, is a leading provider of enterprise learning software applications and related services. This company was founded in 1997, and today has a number of software applications which are used to manage e-learning, transaction processing/e-commerce, and online communities (Blackboard Inc, 2010). For the purpose of the comparison, this university service will be referred to as the 'Primary Service'.
- A service used by a number of departments within the university for a select number of students, which utilises the Moodle software. This software, Moodle, is an Open Source Course Management System (CMS), also known as a Virtual Learning Environment

(VLE). It has become very popular as a tool for creating online dynamic web sites for both instructors and students (Moodle.org, 2010). This application is created and manufactured by a worldwide community of developers. For the purpose of the comparison, this university service will be referred to as the ‘Secondary Service’.

Some of the main features both applications provide are: (1) Content delivery through SCORM packages, lessons and various document formats, (2) Assessment capabilities through the use of quizzes, questionnaires and assignment uploads (3) Collaborative capabilities through the use of forums, chat rooms, wikis and email.

The guidelines provided by the Irish data protection commissioner when considering security of a system, included areas such as access, encryption, antivirus, firewalls, log and audit trails, the human factor, physical security, backups and wireless networks. From this, the researcher decided to compare the two VLE services across the architectural layers of infrastructure, operating system and application. This comparison includes any policy and procedures the services have in place to cater for security and privacy. The comparison is carried out on a point by point scheme so as to ensure any improvements the primary VLE service can make regarding security and data protection are highlighted.

At this stage, it is important to note that all comparisons and conclusions outlined in this study are solely related to the VLE services in use at the university and are not related to the creator/vendor design of the applications.

Infrastructure Layer:

The secondary service is externally hosted while the primary service is managed on-site at the university. Both services have procedures in place for the daily, weekly and monthly onsite and off-site backups of the system data. A test restore policy is also in place for the primary service,

ensuring the integrity of the backups. Redundancy in power supplies and hardware infrastructure is also catered for by both, with the secondary service using RAID 5 array configurations and the primary service using a combination of RAID 5 and RAID 10 for the disk storage. In addition, high availability configurations are in use by the services. Both the onsite and externally hosted data centres provide security systems to ensure only authorized personnel have access to the physical structure of the two VLE services.

Operating System Layer:

The operating system used by the secondary service is the Linux distribution Debian; the primary service uses Microsoft Windows Server. Both services are based on vendor recommendations; however it is important to note that both applications have the capabilities to run on either operating system. The choice of which operating system to use was specific to the university requirements as determined by administrators managing the services. Regular operating system updates and patching are actively applied to both services with clear procedures in place to ensure continued integrity of data during and on completion of an update.

The security protocol, secure sockets layer (SSL) is used by both for all sensitive data transfers. In the case of the primary service, data transfers for account management are involved in the integration of the service with the university Student Information System. Server wide antivirus protection is also used by both, with a centrally managed antivirus service providing the support for the primary service. External monitoring which continually assesses a systems performance and possible issues with security is used by both the secondary and primary services. Reports from monitoring allow administrators to gain valuable insight in the VLE usage and possible areas which may be at risk with regard to security.

Application Layer:

The SSL feature is available in both applications; the secondary service has this functionality in use, while the primary service was in the process of enabling the feature at the time this report was written. With regard to authentication, both applications have the capabilities to be integrated with LDAP/Active Directory services, which allows for existing users of a network to use only the one user id and password. The secondary service currently does not use this authentication method, instead users receive a separate id and password for the service, however the primary service is fully integrated with the university's campus directory, allowing the students to access the system using a single user id and password. Both services have password policies in place and insist on the use of strong passwords. The secondary service achieves this through the application while the primary service has achieved it through the use of the campus directory services, rather than the application.

With regard to security patches directly relating to the application, both vendors make every effort to address security issues promptly, the Blackboard security methodology provides a continuous-feedback loop which caters for new threats and ensures they are quickly identified and prioritized so that countermeasures can be put in place (Saltzman, 2009), while Moodle allows all users to submit bug reports to their bug tracker until they are assessed, only the Moodle security team have the permissions to see those flagged as serious security issues (Berry, 2009). Once patches are released, however the responsibility is with the system administrator to apply to the VLE services. Both services used by the university have processes in place to ensure patches are evaluated and implemented on a regular basis, e.g. the ITIL framework for service and change management, is used by the primary service when applying patches.

User roles within both applications can be configured. The ability to possibly cause disruption to a service, security or another user's privacy, is dependent on the role a user has within the application and as such roles need to be considered an important feature. Each application allows for roles to be set at a system level. Both the primary and secondary services have catered for this, setting student users in a role which only allows them participate in courses they are registered. This limits their account abilities to that of the core functionality of the system and ensures they do not have the ability to manage, influence or hinder other user accounts or data. Access to account and course management is restricted to the administrators of both services.

From an architectural standpoint, both services appear to have implemented the core and most essential areas of security and privacy. However a VLE service does not only consist of a technical architecture; it also contains numerous technical and business processes. Therefore, the researcher decided in order to provide a full evaluation of the services, a comparison was also required of the services against Irish data protection policy. The following outlines the results of the data protection policy comparison.

4.1.2 Data Protection Policy Comparison

For the comparison of the primary service against data protection policy, the researcher decided to reference the data protection guide provided by the office of the Irish Data Protection Commissioner and the privacy guidelines provided by the primary service application vendor, Blackboard. Blackboard inc (2007) provide a privacy document to administrators which outlines information on the United States privacy laws which are relevant to the Blackboard VLE application and specifically the areas of the application which administrators need to examine to ensure compliance of US privacy law. The Irish Data Protection guide, outlines responsibilities

of a data controller who is involved in the collection, storage or processing of personal data in Ireland. This guide includes the main data protection principles for which a data controller or organisation must be in compliance with, under legislation.

This comparison applies the data protection principles against the primary VLE service and where applicable includes an assessment of the processes in place for the service which cater for the areas of the application highlighted by the vendors privacy guide. The eight rules of data protection as stated by the data protection commissioner are detailed below with a point by point scheme used to compare the policy and procedures of the primary VLE service. The objective of the comparison is to highlight any process of the service which needs to be adjusted in accordance to the principles and vendor privacy guide.

The Eight Rules of Data Protection (Dataprotection.ie, n.d.)

1. Obtain and process information fairly

The primary service core data for account and course creation and maintenance is obtained from the University Student Information System, which is considered the authoritative source for all student teaching and learning related data. The primary service only retains data pertinent to the teaching and learning requirements of the student, i.e. identification details for authentication and communication, enrolment details for course evaluation. As such the system complies with the principle.

2. Keep it only for one or more specified, explicit and lawful purposes

Data held by the primary service is for the sole purpose of assessing a students' knowledge with regard to the course they are seeking certification in.

3. Use and disclose it only in ways compatible with these purposes

Only core data of the users identity is portrayed automatically in the primary service, additional details are subject to the user deciding to enter them into the application. Only registered students of the university have access to the primary service and are restricted to accessing only the courses for which they are enrolled. According to the Blackboard privacy guidance documentation the following areas of the application has the ability to disclose a user's personal data, depending on configuration by the administrator. However each role has been reviewed, configured and managed by the current VLE system administrators. The main roles which can come into contact with personal information are listed below with reference made to the processes in place by the primary service to combat any privacy concerns:

- Administrator role – can access personnel data through
 - i. Log files – contain records of specific events and user actions in the system and as such include personal information. Access to the log files of the primary service is restricted to a small number of technical staff whose work is directly related to the management of the environment and service.
 - ii. Snapshot – is a tool provided by Blackboard which enables the ability to bulk create and maintain data from external systems. This tool has the ability to integrate any privacy flags set in the student information system to the VLE application. Within the university environment, access to this tool is restricted to a limited number of technical staff directly involved in the management of the primary service data. However to date the use of privacy flags from the student information system has not been considered or investigated.

- iii. Building Blocks - are commercial or university developed pieces of software which can be added to the VLE application to increase functionality. As such a building block may require access to user's personnel data. Blackboard privacy documentation recommends that administrators only install building blocks which are trusted. The primary service in use by the university uses the ITIL framework for service and change management which ensures any additional pieces of software added to the service are rigorously tested and verified prior to being introduced to the service and user community.
- Course Instructor Role – may access personal data at a course level, this may occur through the use of functionality such as the grade book, contact information and roles within the course. To manage course usage, the primary service has a process in place which requires a lead instructor to initially take ownership of a course, after which the service automatically manages the assignment of the instructor against the course. Removal of the lead instructor from the course requires some intervention by the service administrator. However reviewing the privacy principles and vendors privacy guide, this method for managing instructor assignments is not completely satisfactory and will need to be reviewed.
- Guest and observer roles by default cannot see other user's personal information and as such do not cause any issue regarding privacy or security.

4. Keep it safe and secure

The primary service has disaster recovery, backup and restore, and VLE data management processes in place to ensure data is continually safe and secure.

5. Keep it accurate, complete and up-to-date

Online services allow users to continually update their information; this information is automatically sent to the primary service to ensure user data is continually accurate, complete and up to date.

6. Ensure that it is adequate, relevant and not excessive

Only the minimum amount of information required to authenticate a user, and confirm a user's enrolment in a course, are automatically processed by the primary service. All other information entered into the service, is based on the users own judgement and course requirements which are set by the instructors.

7. Retain it for no longer than is necessary for the purpose or purposes

Data management processes are performed on the primary service to ensure it only contains the most relevant data for current users; this includes scheduled data removal processes to ensure redundant data is not excessive.

8. Give a copy of his/her personal data to an individual, on request

The primary service has processes in place to allow for such requests. However one point which may need reflection is a policy in which the current primary service only holds two years worth of rolling data online and as adoption of the service and years in use increases, it could become a concern for users who have taken a sabbatical and on returning wish to receive their historical data from the service.

4.1.3 Comparative Analysis Conclusion

The analysis of the primary e-learning service against the secondary service and data protection guidelines has shown the overall service to provide the basic and most essential areas

of security and privacy compliance. However a number of minor areas have been highlighted which in the researchers options may need review. The areas highlighted are:

- Investigation into the possible use of a privacy flag in the integration of the e-learning service and Student information service.
- Review of the policy on the data retention within the service, with a further investigation into possible technical archival solutions.
- Review of the processes in place for the assignment of instructors to courses within the service and the continual management of this data.

4.2 VLE Student User Survey

Please note: all references to blackboard within the survey is referring to the primary service provided to the students by the university. Any usability or functionality issues highlighted in the survey questions or data are relating directly to the service provided and/or the VLE administrator's configuration of the application and not to the software provided by the vendor.

4.2.1 Survey Analysis and Result Structure

The survey results are divided into three main sections, they are:

1. Demographics - provides a profile of the type of users who participated in the study.
2. VLE Usability – focuses on the user opinion regarding the usability of the primary service to complete online learning activities.
3. Barriers and Enablers – assesses the functionality of the primary service which may help or hinder the user in completing their online learning activities.

The style of questions used in the survey is:

- Survey Matrix: this question type enables the inclusion of multiple rows of likert questions within a table with column headers included. A survey matrix question type allows for the user to answer a question using a series of agree/disagree or other likert scale type questions in a table (Questionmark, 1997).
- Multiple Choice: the participant selects one choice from a number of possible answers. The user must select a single choice as the answer (Questionmark, 1997).
- Multiple Response: similar to multiple choice except the participant is not limited to choosing one response; they can select none, one or more of the choices offered (Questionmark, 1997).
- Essay question: the participant answers by typing up to 30,000 characters of text. This question type is used to solicit opinions or suggestions on a particular subject (Questionmark, 1997).

The survey was conducted for five weeks, with the earliest survey completed on March 5th 2010 and the last survey completed on April 6th, 2010. A student population circa 15,000 had access to the survey during the time. A total of 2,038 survey submissions were attempted with a total of 1,145 successfully completed. The complete survey question set is available in appendix A.

However for the purpose of this study, only the data most relevant to the research topic is analysed and presented.

4.2.2 Survey Data Presentation:

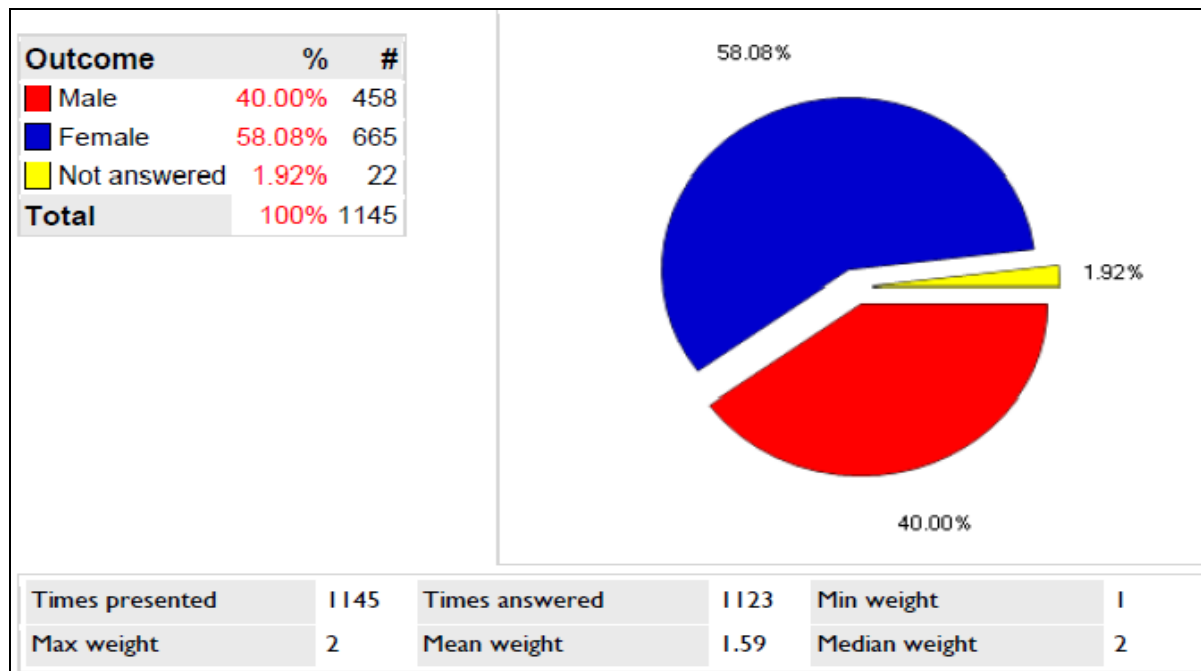
Each survey question is first stated, followed by the categorisation of the question type and the data results which were possible are presented graphically, after which the researcher provides some interpretation of the results, this interpretation was achieved by the researcher aligning the results against the focus of the study.

4.3 User Survey Results

4.3.1 Demographic Profile

Question: What is your gender? , Question type: (Multiple Choice)

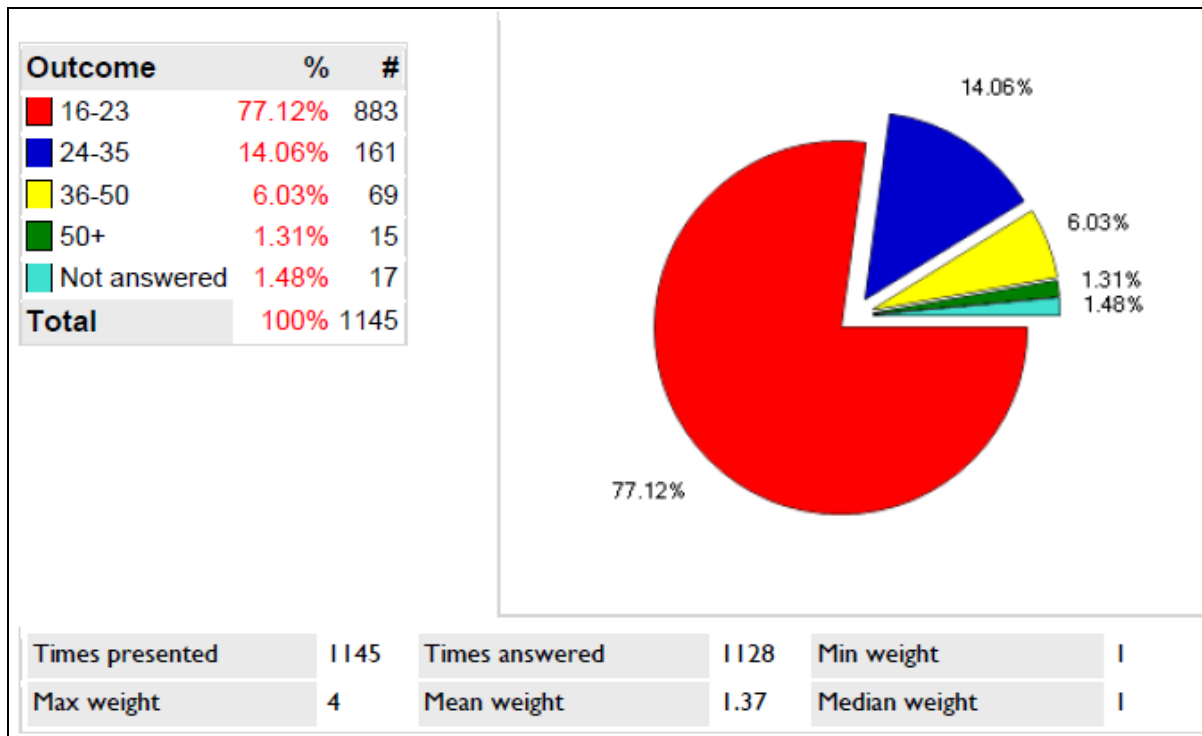
Outcome: Figure 2: Gender Results



Result Interpretation: The results of this question show the demographic of the users surveyed to be a fairly even representation of both genders, with the female population leading slightly by 18.08% or 207 users.

Question: What is your age? , Question Type: Multiple Choice

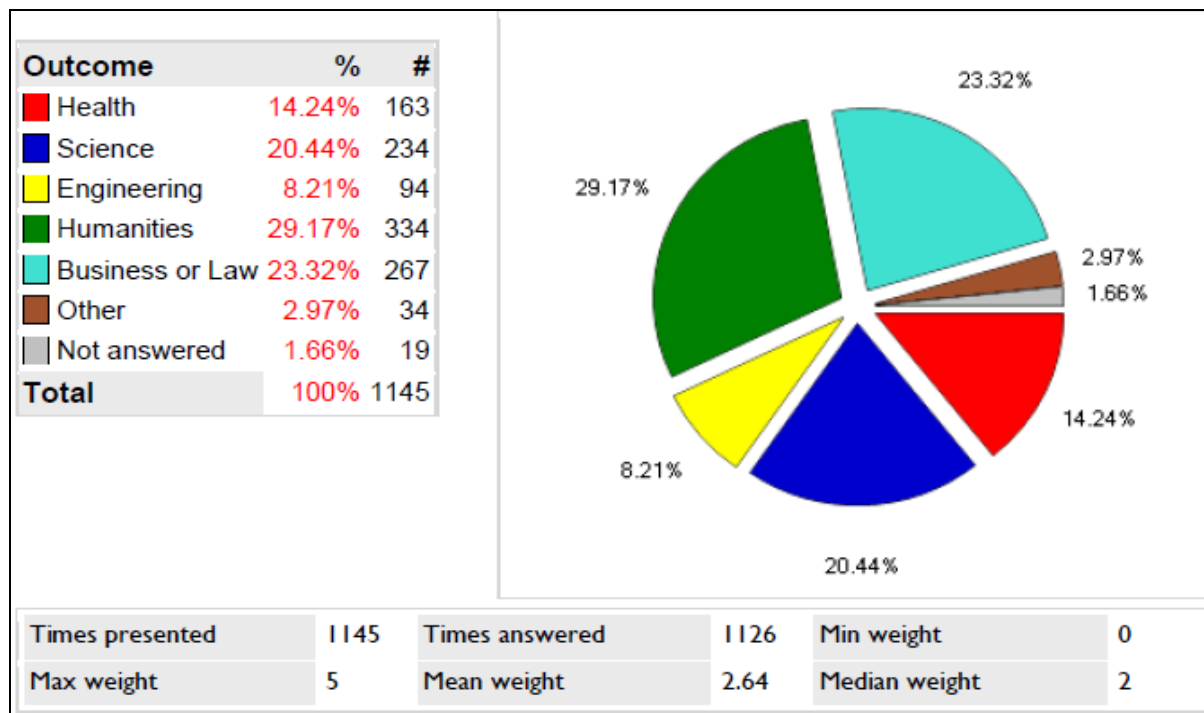
Outcome: Figure 3: Age Results



Result Interpretation: the majority of users completing the survey are within the age bracket of 16-23 years. Considering the target user group was the student population, this result is not that surprising. However it does need to be reflected in the demographics that the student base of the mature student opinions is not significantly represented in the survey and as a result requirements from that group of users cannot be accurately assessed or discussed in this study.

Question: What field are you studying? , Question Type: Multiple Choice

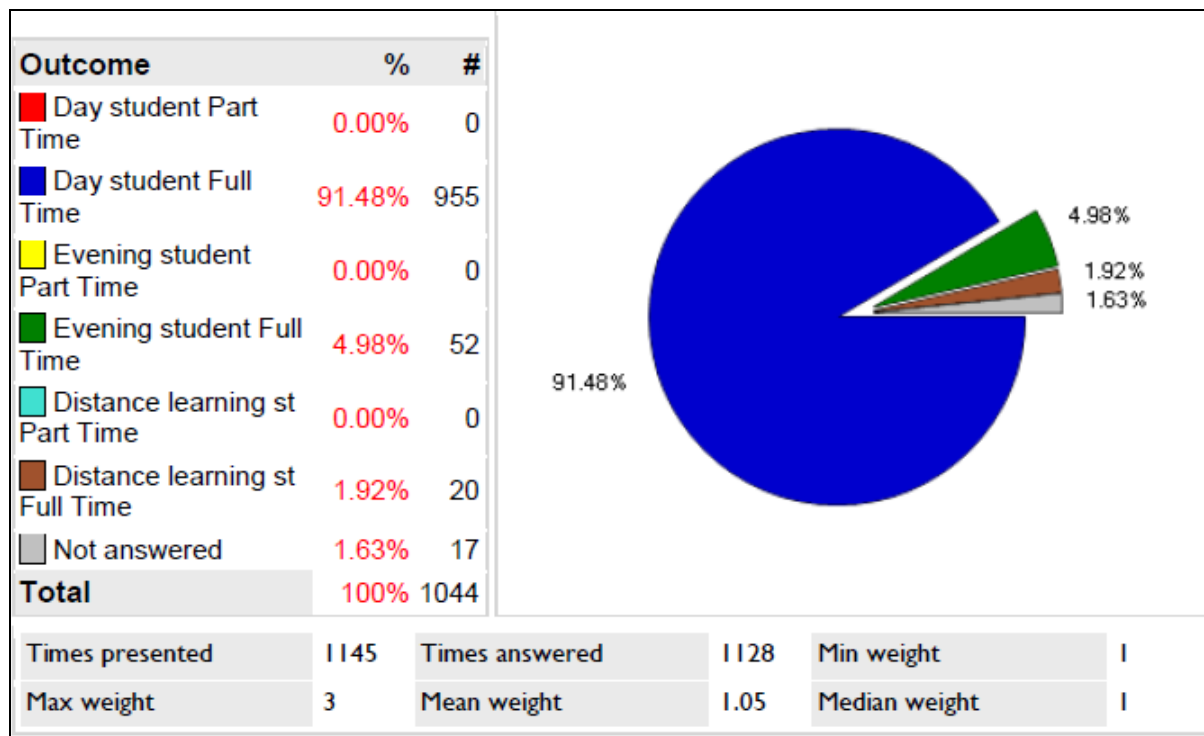
Outcome: Figure 4: Field of Study Results



Result Interpretation: An even representation between three of the areas of study are shown in the results, Science, Humanities and business/Law are the three largest areas of study represented. However it is important to consider that a large number of students study in these areas on a yearly basis within the university and class sizes can generally be smaller in the areas of medicine and engineering. Therefore the results do not provide an accurate way to interpret specific department usage of the primary service or in fact the technical abilities of the users surveyed.

Question: - How do you attend the university? , Question Type: Survey Matrix

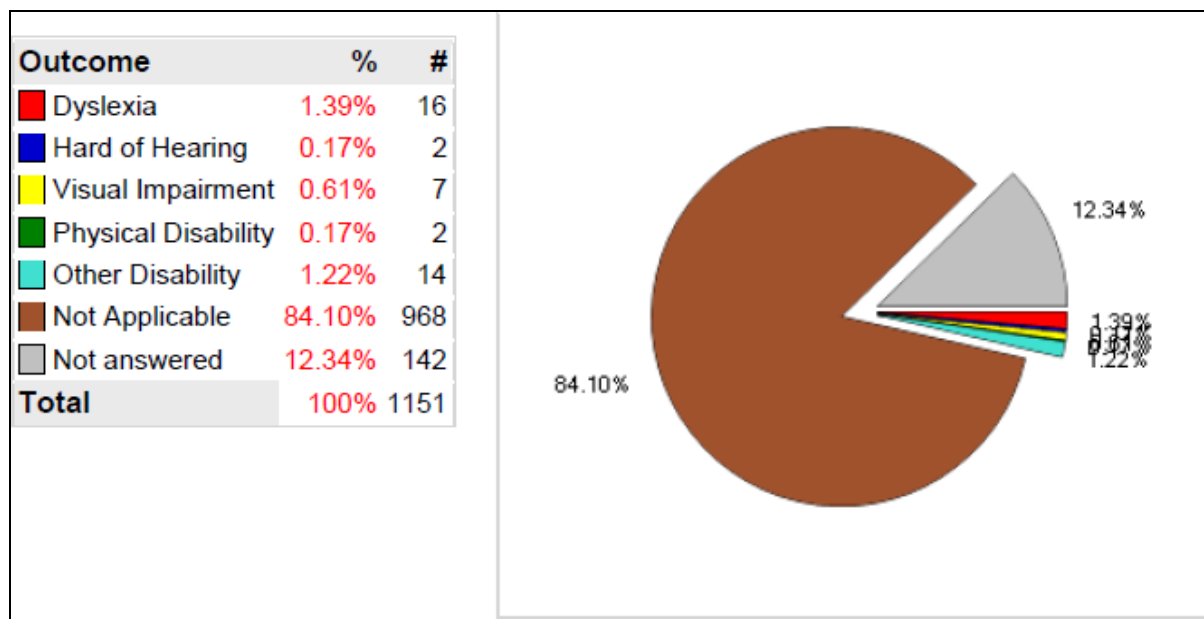
Outcome: Figure 5: Student Type Results



Result Interpretation: with a result of 955 of the 1145 users surveyed being day students attending the university full time, the data presented in the survey can only be considered to represent the requirements for this type of student, with regard to security and privacy within online learning. The representation of evening and distance students is very small and as such will not provide a true reflection of their requirements for this study.

Question: Do you have a disability/learning difficulty that affects your learning experience at the university and your use of Blackboard? Question Type – Multiple Response

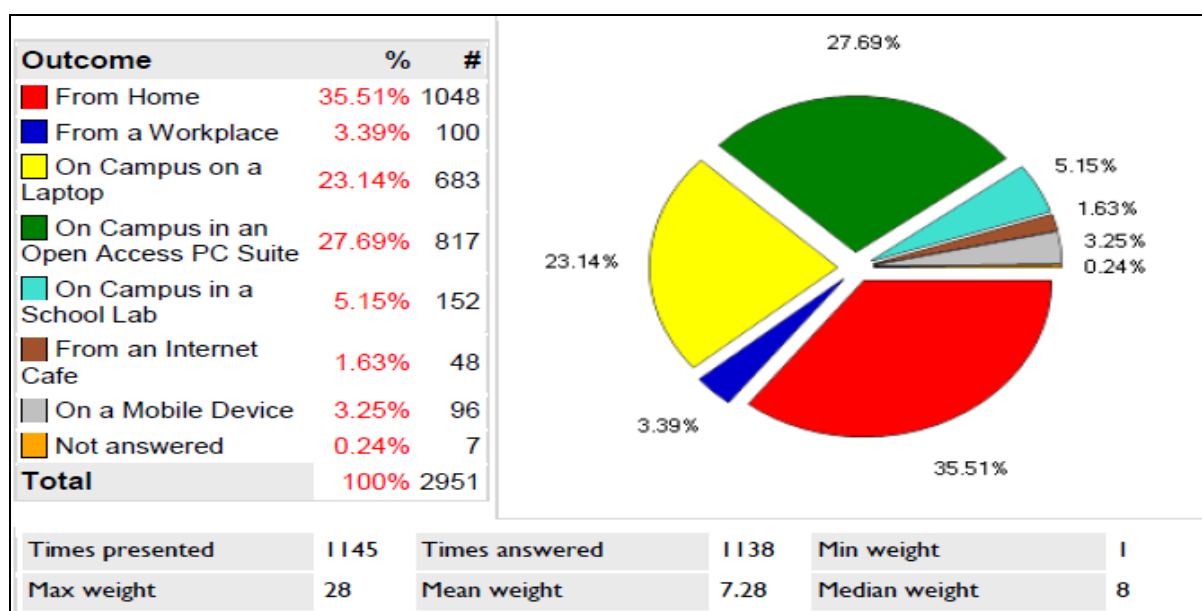
Outcome: Figure 6: Disability Assessment Results



Result Interpretation: the aim of the question was for the researcher to be able to evaluate the primary services ability to cater for a student with a disability. However the results of the survey show the majority of surveyed users do not have a disability and as such the data received cannot be used to accurately present a student with a disability, online learning security requirements.

Question: Where do you access Blackboard from? , Question Type: Multiple Response

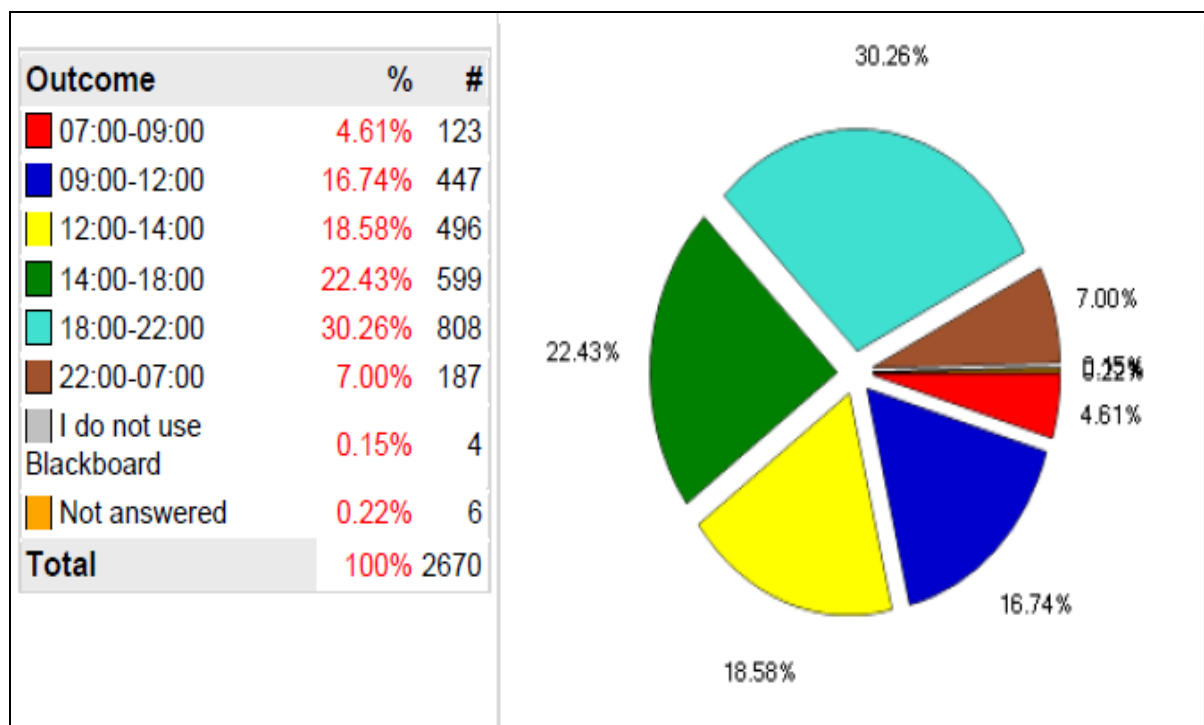
Outcome: Figure 7: Access by Location Results



Result Interpretation: Out of the choices provided, the three top areas for access are, at home, on campus via a laptop and on campus via the student designated pc rooms. Security and privacy requirements of the primary service cannot be accurately assessed based on the location of access provided in this survey. However, the results do highlight the known nature of an e-learning system, which can and will be accessed from anywhere.

Question: At what time do you mostly use Blackboard? , Question Type: Multiple Response

Outcome: Figure 8: Access by Time Results



Result Interpretation: This question shows the flexible nature of an e-learning system and as such shows the security requirements of the users surveyed cannot be assessed on the basis of the time of day they are accessing the system.

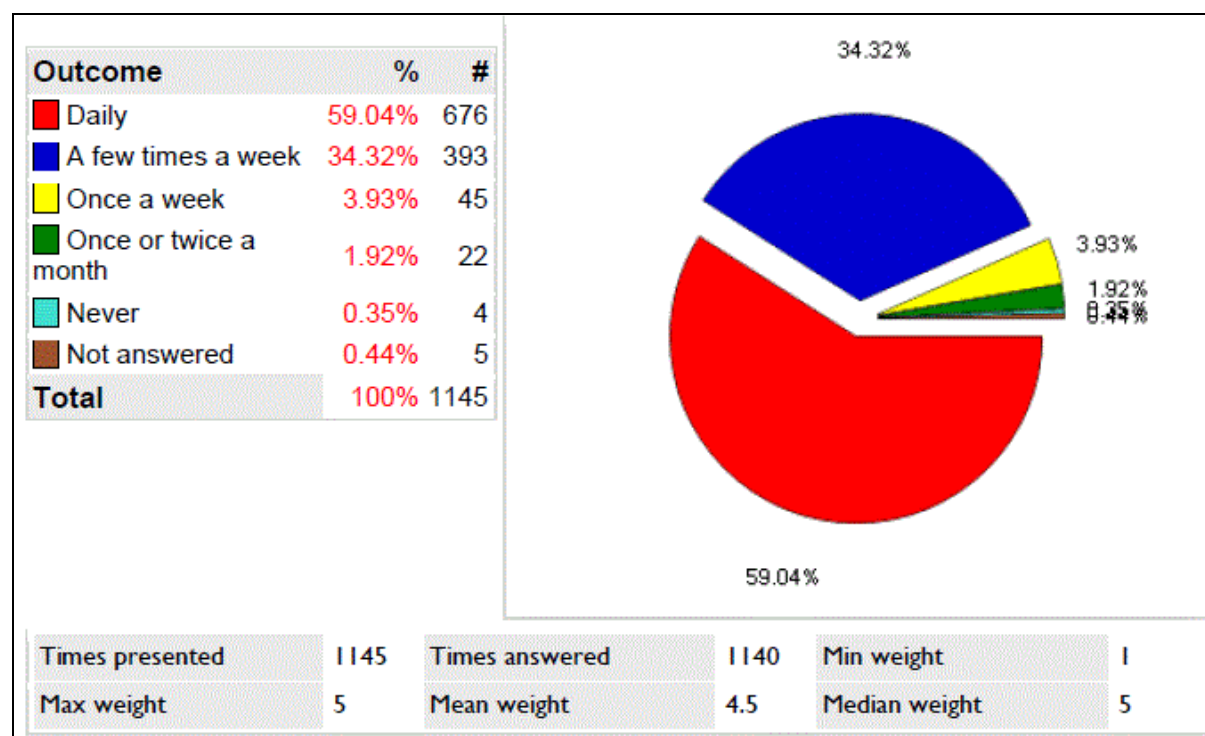
4.3.2 Demographic Summary:

The demographic profile of this survey is that of, a student aged between 16-23 without a disability, who is a day time student, attending the university full time. Although some survey results did represent other demographics of users, i.e. student with a disability, mature student, evening student, etc, in the researcher's opinion, the data set provided was significantly in the minority and therefore would not prove to be an accurate assessment of their requirements.

4.4 VLE Usability

Question: How often do you use Blackboard? , Question Type: Multiple choice

Outcome: Figure 9: Usage Frequency Results



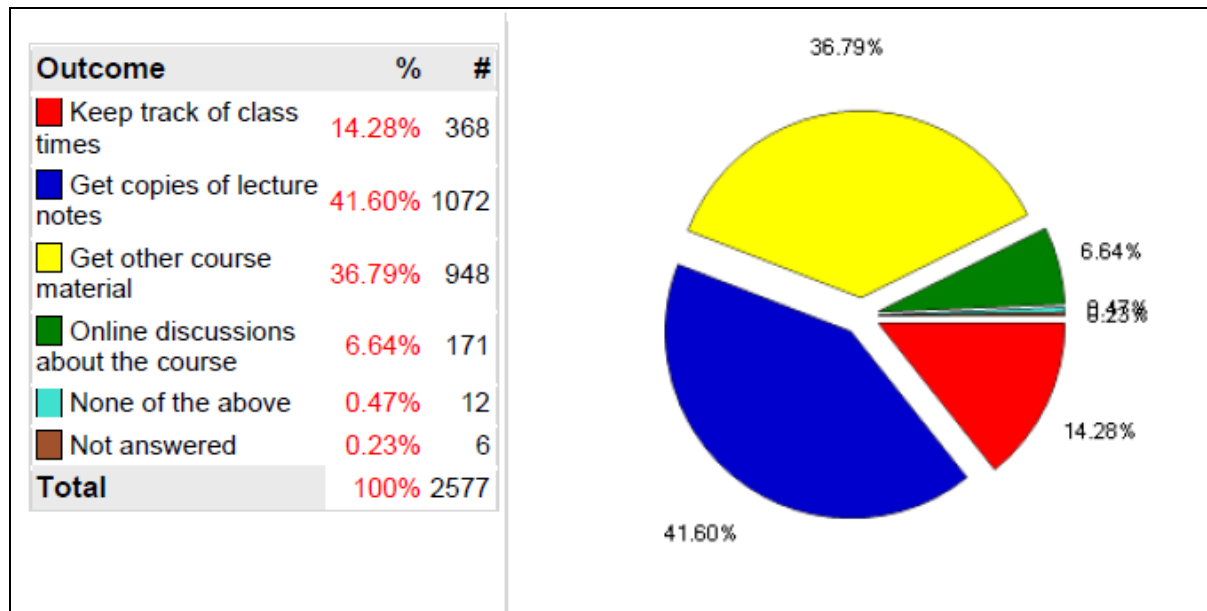
Result Interpretation: A high percentage of the users surveyed use the primary service on a daily basis, with the remaining user's majority, using the system a few times a week. This allows the data represented to be considered accurate in terms of users who actively use the service for

online learning activities. As such, the data should represent a user group, knowledgeable in the primary service functionality and issues relating to their security or privacy.

Question: If you use Blackboard, why? What are the benefits? , Question Type: Multiple

Response

Outcome: Figure 10: Usage Benefit Results



Result Interpretation: the results of this question shows that the users surveyed primarily see the service as a way to access course material, only a small percentage noted the collaborative functionality of discussion boards. This data highlighted to the researcher, what the core functionality of the service is used for. However the results, in fact, don't provide an insight into the user's opinion with regard to the additional functionality available and whether this functionality is deemed to be privacy intrusive or security aware.

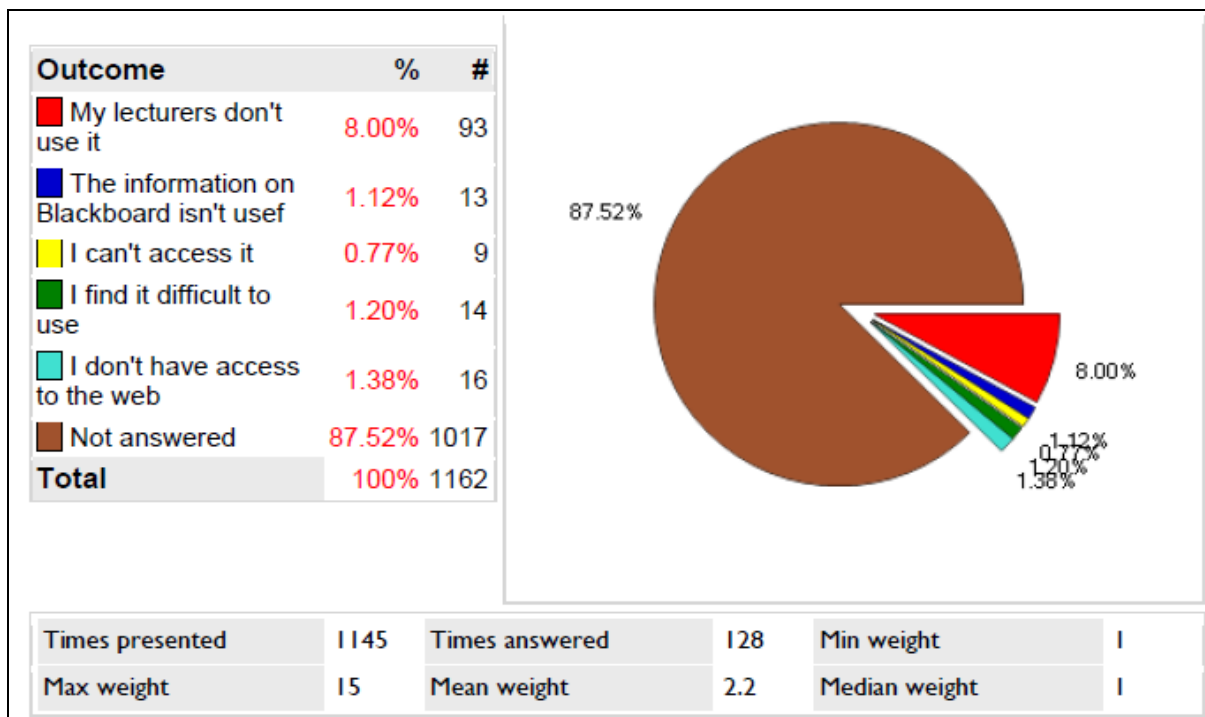
Question: Are there other reasons why you use Blackboard? , Question Type: Essay

Outcome & Interpretation: A total of 662 responses were received for this question. The majority of comments referenced the following reasons for using the service in addition to the areas outlined in the above question, (1) upload assignments, (2) take exams, (3) obtain grade

results, (4) receive announcements, (5) track deadlines, and (6) received course related reading material recommendations. The comments provided the researcher with a view of the core areas in use by the student population in the primary service; as such the data has given the researcher, an insight into specific areas and processes of the service which should be assessed further, with regard to security and privacy.

Question: If you do not use Blackboard, why not? , Question Type: Multiple Response

Outcome: Figure 11: Non-Usage Results



Result Interpretation: majority of users surveyed use the system. For those who don't, the issue seems to be directly related to the structure of their course or the lack of usage of the service by their instructor. Only a minority of users, 3.35%, stated a technical reason for not using the service of which none are security or privacy related.

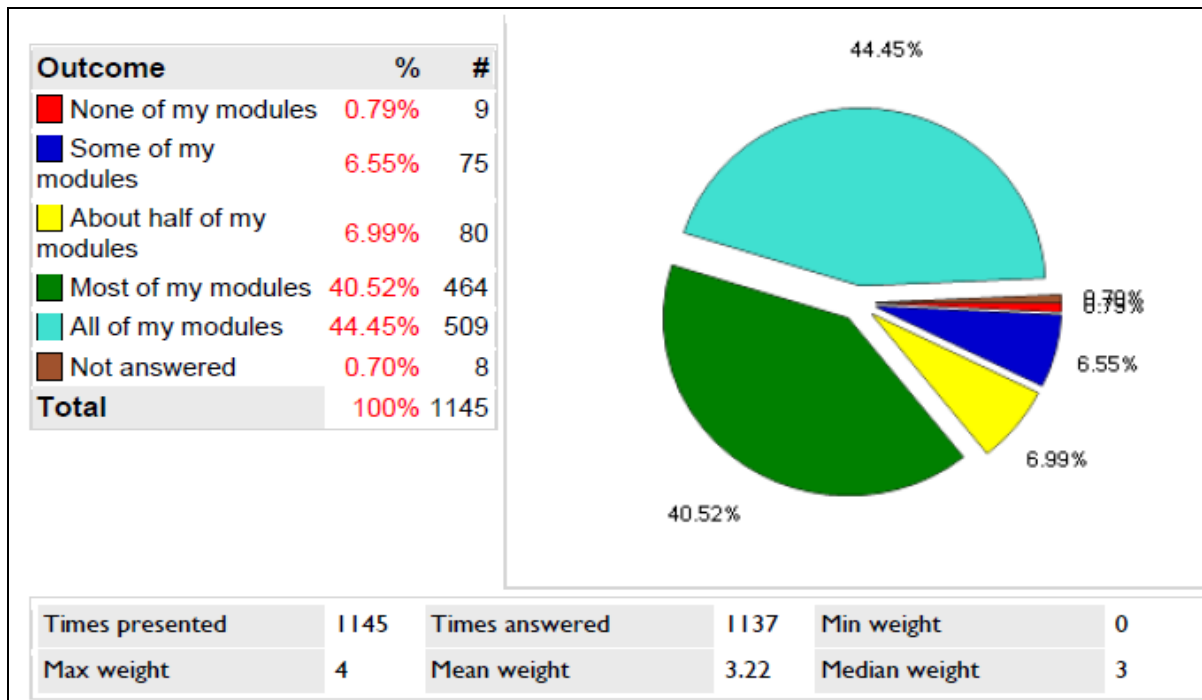
Question: Are there any other reasons why you do not use Blackboard? , Question Type: Essay

Outcome & Interpretation: a total of 124 responses were received for this question. The majority of comments referenced the structure of their course, as the reason for not using the service, i.e. the service was not in use by the course instructors. A minority of users mentioned issues with the ability to easily search and find information within the service and provided suggested solutions relating to the standardisation of formats among courses using the service. Although the results do reflect areas of the course presentations which could be improved, the researcher did not find any comments which reflected a security or privacy related reason for a user not to use the service.

Question: What proportion of your modules this year has had material in Blackboard?

Question Type: Multiple Response

Outcome: Figure 12: Subject Usage Results



Result Interpretation: adoption of the system by the users is high, with the majority of users surveyed, 44.45%, access the system for all their module information and a high percentage of the remainder, 40.52%, accessing most of their modules. This result shows that the primary service is actively being used by both the staff and student community of the university, which implies a positive reflection on the service design with regard to usability. The researcher also considers this data result to be a reflection of the user's confidence in the service and therefore ascertains that security issues or privacy concerns relating to the service must be minimal among the student population.

4.4.1 Barriers and Enablers

Question: Are there other ways, good or bad, that using Blackboard affects your learning?

Question Type: Essay

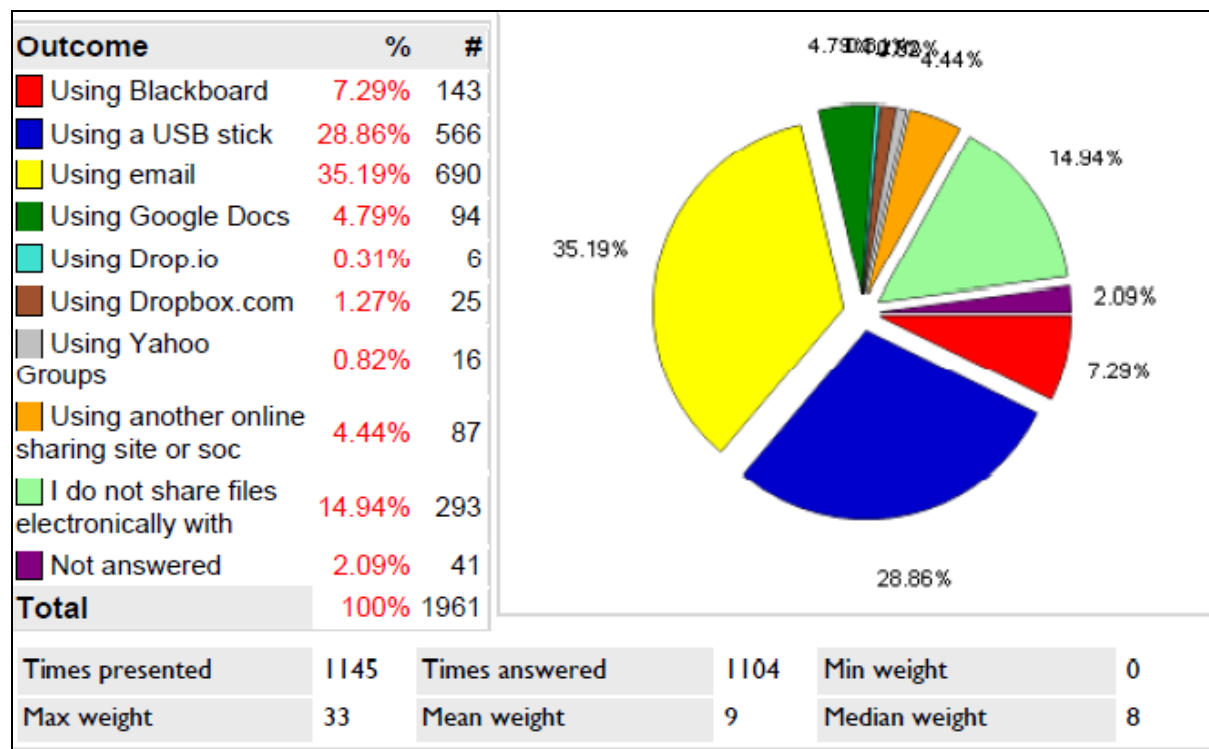
Outcome & Interpretation: a total of 272 responses were received for this question. The highest portion of comments referenced the ease of accessing lecture notes in advance of attending a lecture as being a positive of the primary service. Second to this, the ability to retrieve course instructor contact details through the service was listed as an advantage. A negative highlighted in some of the responses, reflected just the general nature of an online service, as some of the users felt the ability to complete online learning activities were hampered with the ease a user can drift off onto other websites, rather than focusing purely on the learning activity. However this is human nature and not one the service can technically solve. Another negative highlighted was, some responses referenced the service as being used as nothing more than a file hosting service and requested the possibility that the collaborative tools could be further utilised within the service, including the ability to personalise their learning space within the environment to their own needs. This last point is certainly something which can be

improved, from both a software and process level, updates in the software and in some third party building blocks, which are already available provide improved functionality of collaboration tools and personal learning spaces and from a process level a review of how users are alerted to these tools can be carried out. However for the purposes of this study, the comments provided in this section did not raise any concerns or requirements relating to the security or privacy of the data within the service.

Question: Do you ever share files with other students on your course electronically? If so, how?

, Question Type: Multiple Response

Outcome: Figure 13: Electronic File Sharing Results



Result Interpretation: the result of this question is particularly interesting as previously results had referenced the use of the service as a primarily a file hosting service, however the results of this questions shows the majority of users do not share files across the service but rather use methods such as email and USB instead. Therefore the file hosting statement can only be

associated with the files provided by instructors and not the sharing of files between students.

This questions the collaborative design of the current service and the possibility that the role of the student within the service is too restricted. So rather than highlighting a security issue relating to a weakness, the results raise the question whether the current security configuration of the service is too restrictive. Although the application provides numerous ways for collaboration between users, it is obviously the current service is configured to only allow basic collaboration among the university users and possibly should be reviewed.

Question: Please let us know whether you agree or disagree with the following statements:

- I would like to be able to receive Blackboard course notifications and updates on Facebook, (select 'Not Applicable' if you do not use Facebook)
- I would like to be able to use a Blackboard Application to access course notifications or updates using my iTouch/iPhone , (select 'Not Applicable' if you do not own an iTouch or iPhone)

Question Type: Survey Matrix

Outcome: The total number of responses received for the complete question was 2269, of which 14 users (0.62%) opted for the choice “not to answer”. The rest of the responses divided out as follows:

Total number of responses received for the statement of “I would like to be able to receive Blackboard course notifications and updates on Facebook” was 1129. Table 4: Course notification via Facebook Results below shows a further breakdown of the results obtained.

Total number of responses received for the statement of “I would like to be able to use a Blackboard Application to access course notifications or updates using my iTouch/iPhone” was

1126. Table 5: Course accessibility via iPhone application below shows a further breakdown of the results obtained.

Table 4: Course Notifications via Facebook Results

Outcome	%	#
Agree	17.45%	396
Neutral	9.78%	222
Disagree	17.45%	396
Not Applicable	5.07%	115

Table 5: Course Accessibility via iPhone/iTouch Results

Outcome	%	#
Agree	16.26%	369
Neutral	5.99%	136
Disagree	5.29%	120
Not Applicable	22.08%	501

Result Interpretation: The course notification via facebook has an even number of users who agree/disagree with the introduction of their course material into their personal social networking site. As it stands the 50/50 divide may just show, the topic of integrating is relatively new and as such users have no real bases for a strong opinion. Therefore, it would only be through the introduction of such a service on a pilot basis, that the researcher would be able to obtain further data from the users of the repercussions relating to privacy and security of such an integration.

With regard to the course accessibility via an iPhone/iTouch, the results show for users who own such a device, the choice would be to use an application via the phone to access their course material, with 16.26% of the users in agreement. However the majority of users surveyed don't in fact own such a device at this point in time, with 22.08% surveyed selecting "not applicable".

Question: If you could change one thing about how Blackboard operates, or how it is used by staff, what would that be? , Question Type: Essay

Outcome & Interpretation: A total of 578 responses were received for this question. The results obtained presented some interesting comments, with a high portion relating to the management of grades, submission of assignments and exam related experiences.

However rather than security and privacy related concerns, the users focussed on the reliability of the service when completing assignments or exams. Reliability described in this case was not the service availability but rather users having doubts the submitted work would be received by the instructor in a correct format, within the time frame permitted. No specific functionality is referenced, but rather the processes and policies relating to the submission of work. Interestingly although 578 responses were received, only 5 related to possible security or privacy concerns. The five in particular made specific references to grade notifications within a course; however the issue raised was not related to the grade functionality of the services but rather the instructors chosen methods of making the information available. From this feedback, the researcher has ascertained a review of the exam/assignment submission processes and recommendation regarding grade display should be reviewed.

Question: Please let us know your thoughts, by choosing yes, no or not applicable for each of the following:

- Have you ever taken an Multiple Choice Quiz exam through Blackboard?
- Would you like to take Multiple Choice Quiz exams through Blackboard in the future?
- Have you ever submitted assignments (essays, projects) using Blackboard?
- Would you like to submit assignments using Blackboard in the future?
- Have you ever accessed your provisional grades through Blackboard?
- Would you like to access your provisional grades through Blackboard in the future?

Question Type: Survey Matrix

Outcome & Interpretation: The number of surveyed users who did not respond to the question and instead selected the ‘not to answer’ was 15 (0.22%). The total number of responses received for the complete question was 6790. The high number is related to the number of questions each user needed to answer within the main question. The total number of responses received per question was:

The statement “Have you ever taken a Multiple Choice Quiz exam through Blackboard?” received a response of 1130. Table 6: User Familiarity of Exam Functionality below shows a further breakdown of the results obtained.

Table 6: User Familiarity of Exam Functionality

Outcome	%	#
Yes	9.34%	634
No	6.67%	453
Not Applicable	0.63%	43

Result Interpretation: although the primary service policy is not to support the online exam functionality for users. The survey results show the tools are actively being used, with 9.34% of

the users having already completed exams within the service. As such, a review of the service policy needs to be conducted, with both privacy and security recommendations being considered. The statement “Would you like to take Multiple Choice Quiz exams through Blackboard in the future?” received a response of 1128. Table7: User Interest in using Exam Functionality below shows a further breakdown of the results obtained.

Table7: User Interest in using Exam Functionality

Outcome	%	#
Yes	11.65%	791
No	3.45%	234
Not Applicable	1.52%	103

Result Interpretation: the results of this question, further strengths the researchers recommendation of the exam functionality review within the service, as the majority of users (11.65%) surveyed have stated they would like to use the service for completing exams, while in comparison only 3.45% surveyed declined.

The statement “Have you ever submitted assignments (essays, projects) using Blackboard?, received a response of 1130. Table 8: User Familiarity of Assignment Submission Functionality below shows a further breakdown of the results obtained.

Table 8: User Familiarity of Assignment Submission Functionality

Outcome	%	#
Yes	13.20%	896
No	3.09%	210
Not Applicable	0.35%	24

Result Interpretation: results show the assignment tool to be actively used among the student population and as such the functionality and policy around assignment submission should be reviewed. Currently the use of this tool is primarily left to the instructor and any policy relating to missing or incomplete assignments is left to the instructor to solve. However considering the high usage of the assignment submission functionality, it would be the researcher's recommendation that the administrators of the service review the assignment submission practice to see if improvements can be made.

The statement "Would you like to submit assignments using Blackboard in the future?" received a response of 1130. Table 9: User Interest in using Assignment Submission Functionality below shows a further breakdown of the results obtained.

Table 9: User Interest in using Assignment Submission Functionality

Outcome	%	#
Yes	13.45%	913
No	2.44%	166
Not Applicable	0.75%	51

Result Interpretation: The results show a high interest (13.45%) within the user base of using the assignment submission functionality, while only a minority of the users disagree (2.44%). This result set only strengthens the researcher's recommendations of a service review of the assignment submission process, as mentioned in the interpretation above.

The statement “Have you ever accessed your provisional grades through Blackboard?” received a response of 1130. Table 10: User Familiarity of Accessing Provisional Grades Online below shows a further breakdown of the results obtained.

Table 10: User Familiarity of Accessing Provisional Grades Online

Outcome	%	#
Yes	11.93%	810
No	4.24%	288
Not Applicable	0.47%	32

Result Interpretation: 11.93% of the users have already obtained their provisional grades through the service, while only 4.24% have not. Again, the results for accessing provisional grades online, shows a user community endorsing the use of the service for all online learning activities.

The statement “Would you like to access your provisional grades through Blackboard in the future?” received a response of 1127. Table 11: User Interest in Accessing Provisional Grades Online below shows a further breakdown of the results obtained.

Table 11: User Interest in Accessing Provisional Grades Online

Outcome	%	#
Yes	15.13%	1027
No	0.97%	66
Not Applicable	0.50%	34

Result Interpretation: An overwhelming 15.13% (1027 users) surveyed would like to access their provisional grades online. Taking into consideration this result and the results of the essay comments of earlier questions, relating to the usability of the service; it is clear to the researcher that the user community is embracing the service of online learning with little to no concerns regarding the security or privacy of the data. As a result of these findings, the researcher will be recommending a review of the grade centre functionality within the service and the methods by which instructors are using to notify users of their grades. With a view to producing guidelines of how the functionality can be used and the technical methods recommended for grade notifications.

Question: Currently, each course on Blackboard is accessible only to registered students and those involved in the delivery of that course (academic staff and/or tutors). Do you agree with this policy? , Question Type: Survey Matrix

Outcome & Interpretation: As Users may not have completely understood the basis of the policy, three subset statements were made and the users were asked to provide an opinion by selecting one of the following for each statement, Agree, Disagree, Neutral, Not Applicable. The subset of statements was:

- I would like only registered students to have access to my courses on Blackboard.
- I would like anyone (at the university) to have access to my Blackboard modules.
- I would like anyone (anywhere on the internet) to have access to my Blackboard modules.

A total of 1129 responses were received for each statement, with only 16 users opting to not answer the question. A breakdown of the results is provided in the three tables below, note the results of the statement I would like only registered students to have access to my courses on

Blackboard, are detailed in Table 12: Registered Student Only Access Results; I would like anyone (at the university) to have access to my Blackboard modules. Are detailed in Table 13: All University Personnel Access Results and I would like anyone (anywhere on the internet) to have access to my Blackboard modules are detailed in Table 14: Anyone/Anywhere Access Results. .

Table 12: Registered Student Only Access Results

Outcome	%	#
Agree	24.44%	815
Neutral	5.49%	183
Disagree	3.42%	114
Not Applicable	0.21%	7

Table 13: All University Personnel Access Results

Outcome	%	#
Agree	6.66%	222
Neutral	8.01%	267
Disagree	18.08%	603
Not Applicable	0.30%	10

Table 14: Anyone/Anywhere Access Results

Outcome	%	#
Agree	2.79%	93
Neutral	3.72%	124

Disagree	26.18%	873
Not Applicable	0.24%	8

Result Interpretation: The aim of this question was to assess the user's concepts of data privacy within the world of online learning. So as to assess the user requirements, the researcher wanted to first assess whether the concept of protecting ones data was consciously considered by the user. The results show that although the users have actively embraced the role of online learning in their university life, they are equally conscious of protecting the data from a wider audience than the registered students of the university, with 24.44% of the users surveyed agreeing to share their course data. However, the results show the user community completely against sharing their online course with people outside the realm of registered students for the course, with 18.08% disagreeing with allowing additional personnel of the university access and 26.18% disagreeing with additional internet users having access.

4.4.2 Survey Conclusion

The user requirements gathered from the survey with regard to security and privacy are not extensive. The results showed the user community to have completely embraced the nature of online learning and reference little to no issues with the service in regard to security or data protection. The areas that were highlighted by the users as actively used and therefore a required focus for security and data protection were: (1) Assignment submission, (2) Online exams and (3) accessibility of provisional grade results. From this, two main requirements were assessed:

1. For each of these areas, the users have stressed the need for assurance in the reliability of the service to manage and protect the information. Suggestions as simple as electronic receipts as proof of assignments submitted and recommendations on methods used to

notify users of the availability of provisional grades were made. Therefore one requirement of the users determine by the survey is the provision of a secure, reliable and informative service within the primary e-learning service for completing exams, assignments and receiving provisional grades.

2. A second requirement highlighted from the survey results, is the request by users to have the ability to fully utilise the collaborative tools available within the service. Currently the users feel unable to easily access the collaborative services available within the e-learning service. The issue may be related to the user's role within the service and such a review would be advisable.

5 Chapter 5 – Project History

The following chapter provides a review of how this research progressed, including an insight into some of the decisions and actions which altered the outcome of the study.

5.1 Introduction

For the past five years the researcher has been involved in the technology behind the online learning activities of one of Ireland's main universities. On implementing a virtual learning environment (VLE) solution a University will automatically ensure the VLE hardware, software, database and communication systems are robust and certainly secure from a physical and organizational stand point.

However following the successful launch of the University's primary VLE, the researcher started to consider the value of the data the VLE system would hold and ways in which it could be compromised. Questions relating to online activities and security continued to invade the researcher's thoughts and eventually evolved in to a question of "how many universities take the time to analyze the data security and protection of their VLE environments?"; as a result of these questions , this research topic was created. Initially, research into the topic began in the autumn of 2008, following approval from the Regis University Advisor. However due to a number of circumstances the researcher was prevented from completing the study at that time and resulted in a deferral for the year. The research into this topic re-commenced in the autumn of 2009.

5.2 The Research Approach

As outlined in Chapter 3 – Methodology, the qualitative research design of a case study was selected for this study and the Irish university where the researcher worked was chosen as the case. The university had just completed an intensive upgrade of a piloted VLE system to a

mainstream online learning service. This service was now provided to all staff and students of the university. The university has a student population circa of 15000 and a staff population circa of 3000 and as such the researcher believed would provide this study with an excellent source of fresh data regarding online learning activities and security.

The six steps used when performing a case study as outlined by Soy (1996), were followed to complete this study. One of the first steps performed by the researcher was a review of existing literature on topics relating to online learning activities and data security. This research was carried out over the winter months of 2009. Numerous journals and articles were found and an annotated bibliography created followed by the Chapter 2 – Literature review. One of the main discussions highlighted in the majority of papers was the difficulty encountered by both administrators and users of VLE type environments in finding a balance between the restrictive nature of security and the collaborative nature of an online learning environment.

5.3 Research Objectives

The objectives for this study were to examine the need to meet emerging security requirements for online learning activities within the Virtual learning Environments (VLE) of an Irish University. With the research primarily focus on the following areas:

- A comparative analysis of the security features of the two main VLE's in use by the university.

To complete this objective the researcher defined two stages of the VLE comparison:

1. Comparison of the VLE based on Architecture and security features.

As two VLE systems were in use within the university, it was decided a comparison of their architectures and security features would be carried out, with the hope that any improvements to the architecture with regard to security and data

protection would be highlighted. The original goal was to use a questionnaire format to retrieve the system details, however through correspondence with the system administrators, the researcher realized that the information required was already available through existing literature of both systems. This literature provided the researcher with enough information to accurately complete the comparison of the architecture without the need for a questionnaire. This comparison was carried out during the spring/summer months of 2010.

2. Comparison of the VLE based on University & Irish data protection policy and guidance.

To assess purely on architecture and software design was considered by the researcher to be limited in aiding the discussion of data protection and the universities VLE. So a decision was made to include a comparison of the VLE processes against the data protection policy of the university and the Irish data protection commissioner guides.

This comparison was also carried out during the spring/summer months of 2010.

- A survey of user feedback regarding security components of the existing VLE's on campus, which will help in determining the security requirements of the university. The following decisions need to be made:

1. What was the focus of the study?

One of the main discussions highlighted in the majority of papers was the difficulty encountered by both administrators and users of VLE type environments, in finding a balance between the restrictive nature of security and the collaborative nature of an online learning environment. From the review of literature, the researcher decided to focus the survey on the user's experiences of using the VLE and their expectations on

functionality and concerns they may have regarding their privacy and security when using it. It was hoped this focus would allow the researcher to determine the VLE user's concept of security with regard to online learning activities.

2. What tools would be used to manage the survey development and data analysis

The survey tool selected was Questionmark Perception, which was in use by the university. This tool provided the researcher with a way to analyze the survey data in a graphical format, frequency analysis for multiple choice questions, and a listing of answers for text questions. Questionmark catered for the need to be able to collect and analyze data in an organized manner and as such proved to be a very useful tool. Further details on the software is available at: <http://www.questionmark.com/uk/perception/>

3. Which user base would the survey target

The Blackboard VLE service which had recently been upgrade to a mainstream service was selected and the student users as the target user group. Although a second VLE install (Moodle) is in use within the university, it caters for a smaller number of users and as such would have limited the extent of user survey feedback.

4. When the survey should be performed.

The survey was sent out to users for completion over the spring months of 2010, while students are actively attending the university. This was in the hope of getting a large number of responses from the user community.

- An analysis of available security technologies in relation to standards, which will lead to a recommendation on how these security technologies, can meet the requirements of the university.

This objective was based on time permitting within the study to complete a review of new security technologies which could be applied to the VLE. Considering the review of literature, extent of survey data collected and the level of comparative analysis involved, the researcher decided it would be prudent to fully ascertain the VLE user concepts of security and there interaction with the VLE, prior to assessing new technologies which would lead to a change to the VLE architecture. Instead the researcher decided to add this objective as a recommendation to the university, such that analyses of emerging new security technologies are carried out, to meet the security requirements determined.

5.4 Conclusion

Once the evaluation of the VLE user survey data and assessment of the current configuration of the primary VLE with regard to data protection was completed, the researcher was able to ascertain the security requirements and propose recommendations for the Irish University and as such complete the study.

6 Chapter 6 – Conclusions

The following chapter provides a summary of the study findings, and outlines the challenges encountered. In addition some suggestions are provided of future research areas.

6.1 Introduction

The following chapter is divided into four sections. First, the conclusion section presents a summary of the study findings. This is followed by the section on the contribution this study has made to the research community. After which a section on lessons learned is provided to give an insight into issues encountered by the researcher during the conduction of the study. The final section relates to future areas of research that could be explored.

6.2 Study Conclusion

Chapter Four - Analysis and Results, detailed the findings of the researcher following the completion of the review of the survey data and assessment of the e-learning services. The findings can however be divided into two summarised sets, they are (1) User security requirements of the existing e-learning service and (2) Recommendations of how the university can meet the user requirements.

1. User security requirements of the existing e-learning service

- The collaborative tools of the service need to be easily accessible by the student user community.
- The online exam services within the e-learning service need improved reliability.
- The assignment submission process within the e-learning service needs to expand informational messages to provide assurance to the user of successful submission.
- The methods used to provide notification of provisional grades within the e-learning service need to be standardised.

2. Recommendations of how the university can meet the user requirements.

Based on the requirements gathered and the results of the e-learning analysis, the researcher has produced the following recommendations.

- A review of the online exam and assignment submission service policy and performance. With a recommendation of an investigation into additional technologies and processes which will improve the reliability and usability of the services.
- A review of the student role within the service, with the aim of improving the accessibility of the collaborative tools among the student population.
- An investigation into possible archival solutions for the eventual historical data the service will hold.
- A review of the processes used to manage the assignment of instructors to their relevant courses within the e-learning service, with the aim to determine a single authoritative source for which the data can be managed.
- A technical assessment of the integration of the e-learning service with the student information services, to evaluate the possible use of privacy flags.

6.3 Contribution

This study has provided some user security requirements within an e-learning service of an Irish university and as such will hopefully provide other universities and e-learning services with a guide to the interaction of a user community and their online service. In addition the data collected throughout the study will contribute to the discussions on e-learning services and security.

6.4 Lessons Learned

The main issue encountered by the researcher was in the area of gathering the requirements from the user community. Although the researcher wanted to evaluate the users opinions of security and privacy within the service, consideration needed to be given to ensuring the users continued confidence in the service and that concern relating to the security of the service was not raised. Therefore the design of the survey, and in particular, the format of the questions was crucial. In fact, it is only on the return of survey data, does one fully realise the potential of additional questions which could be asked. From this, one of the main lessons learned by the researcher is to narrow the scope of a survey. In addition to this is the user group targeted, although the student population was selected, the survey results only reflected one student demographic and to expand on the user requirements, further surveys of other demographics will be required.

6.5 Future Research

From the review of existing literature and the completion of this study, it is apparent that future research is of extreme importance to the topic of e-learning and security. From the researcher's perspective, an expansion into the research of the user's requirements regarding online exams will be an outcome of the study. For the wider community, future research in evaluating the human interaction with e-learning services and their concept of the need for security and data protection is vital. To truly develop the systems to cater for the user's needs, the needs of the user must be fully understood.

References

- Berry, Miles. (2009). *Moodle and Open Source Security*. Retrieved February 18, 2010, from <http://opensourceschools.org.uk/moodle-and-open-source-security.html>
- Blackboard Inc. (2007). *Blackboard Academic Suite and Privacy*. Retrieved February 08, 2010, from <https://behind.blackboard.com/s/sysadminas/refcenter/docs/details.Bb?DocumentID=3357&pid=100&rid=5759&dt=>
- Blackboard Inc. (2010). *What we do*. Retrieved July 01, 2010, from <http://www.blackboard.com/Company/What-We-Do.aspx>
- Borcea-Pfitzmann, Katrin., Liesebach, Katja., Pfitzmann, Andreas. (2005). *Establishing a Privacy-Aware Collaborative eLearning Environment*, Proceedings of the EADTU Annual Conference 2005. Retrieved January 29, 2010 from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.5166&rep=rep1&type=pdf>
- Cárdenas, Roberto Gomez., Sanchez, Erika Mata. (2005). *Security Challenges of Distributed e-Learning Systems*, ISSADS 2005, LNCS 3563, p538–544. Retrieved January 25, 2010, from <http://www.springerlink.com/libgate.library.nuigalway.ie/content/42xu6r68k8thmw2y/fulltext.pdf>
- Charlesworth, A. (2008). *Code of Practice for the Further and Higher Education Sectors on the Data Protection Act 1998*. Retrieved 11 October 2008 from http://www.jisclegal.ac.uk/publications/DPACodeofPractice.htm#_Toc197501974

Dataprotection.ie. (n.d.). *Data Protection Acts 1988 and 2003, a Guide for Data Controllers*.

Retrieved February 25, 2010, from

<http://www.dataprotection.ie/documents/forms/NewAGuideForDataControllers.pdf>

Gong, Guo-quan., Qiang, Shuang., Wang, Jun.(2009). *Information Security Measures and Regulation Research, 2009 International Conference on Management Science & Engineering*. Retrieved February 26, 2010 from

<http://www.ieeexplore.ieee.org.libgate.library.nuigalway.ie/stamp/stamp.jsp?tp=&arnumber=5317613>

Ingerman, Bret. L., & Yang, Catherine. (2010, May/June). *Top-10 IT issues 2010. Why it matters to Higher Education EDUCAUSE Review*, 45, 46-60

Key, James. P. (1997). *Research Design in Occupational Education*. Retrieved August 10, 2010, from <http://www.okstate.edu/ag/agedcm4h/academic/aged5980a/5980/newpage21.htm>

Leedy, P. D., & Ormrod, J. E. (2005). *Practical Research: Planning and Design (8th Ed.)*. Upper Saddle River, NJ: Pearson Education.

Mwakalinga, Jeffy., Kowalski, Stewart., Yngström, Louise. (2009). *Secure E-learning using a Holistic and Immune Security Framework, Internet Technology and Secured Transactions, ICITST 2009*. Retrieved February 2, 2010, from

<http://www.ieeexplore.ieee.org.libgate.library.nuigalway.ie/stamp/stamp.jsp?tp=&arnumber=5402508>

Moodle.org, (2010). *What is Moodle*. Retrieved July 01, 2010, from <http://moodle.org/about/>

Questionmark. (1997). *Question Types*. Retrieved July 30, 2010, from

http://www.questionmark.com/us/perception/authoring_windows_qm_qtypes.aspx

Saltzman, Matthew. (2009). *Blackboard Security Statement*. Retrieved February 08, 2010, from

<http://kb.blackboard.com/display/KB/Blackboard%20Security%20Statement?sso=34D719C7FBECCCC190BA742DFA637CBF2084994CA3DFFB03F8A7A50CE33D86C9E89B8A8F4CB5CD5E>

Shuttleworth, Martyn. (2008). *Qualitative Research Design*. Retrieved August 10, 2010, from

<http://www.experiment-resources.com/qualitative-research-design.html>

Soy, Susan. (1996). *The Case Study as a Research Method*. Retrieved August 10, 2010, from

<http://www.ischool.utexas.edu/~ssoy/usesusers/l391d1b.htm>

Yin, Robert. K. (2004). *Case Study Methods*. Retrieved August 10, 2010, from

<http://029c7c0.netsolhost.com/Docs/AERAdraft.pdf>

Appendix A

Blackboard Student Survey 2010

Please note: all references to blackboard within the survey is referring to the primary service provided to the students by the university. Any usability or functionality issues highlighted in the survey questions or data are relating directly to the service provided and/or the VLE administrator's configuration of the application and not to the software provided by the vendor.

Q1 of 34 - How often do you use Blackboard?

- Daily
- A few times a week
- Once a week
- Once or twice a month
- Never

Q2 of 34 - If you use Blackboard, why? What are the benefits to you? (Tick all that apply)

- Keep track of class times
- Get copies of lecture notes
- Get other course material
- Online discussions about the course
- None of the above

Q3 of 34 - Are there other reasons why you use Blackboard?

Q4 of 34 - If you do not use Blackboard, why not? (Tick all that apply)

- My lecturers don't use it
- The information on Blackboard isn't useful
- I can't access it

- I find it difficult to use
- I don't have access to the web

Q5 of 34 - Are there any other reasons why you do not use Blackboard?

Q6 of 34 - What proportion of your modules this year has had material in Blackboard?

- None of my modules
- Some of my modules
- About half of my modules
- Most of my modules
- All of my modules

Q7 of 34 - How useful is Blackboard for accessing the following:

- Class Announcements
- Lecture Notes/Handouts
- Other Course Documents
- Reading Lists and Recommended Websites
- Online Discussions
- Quizzes
- Plagiarism Detection (Turnitin)
- Submitting Assignments
- Wikis or Blogs

Q8 of 34 - Are there any other features in Blackboard that you find useful?

Q9 of 34 - In your opinion, is the information placed on Blackboard by your lecturers generally

(tick as many as apply)

- Excellent - couldn't ask for more

- Good- some are great, others less so
- Fair- mostly bare, minimum handouts
- Poor - generally of little use
- Not applicable

Q10 of 34 - For your lecture notes, do you:

- Access them before class
- Print them and bring them to class
- Access them after class

Q11 of 34 - Where do you access Blackboard from? (Tick all that apply)

- From Home
- From a Workplace
- On Campus on a Laptop
- On Campus in an Open Access PC Suite
- On Campus in a School Lab
- From an Internet Cafe
- On a Mobile Device

Q12 of 34 - At what time do you mostly use Blackboard? (Tick all that apply)

- 07:00-09:00
- 09:00-12:00
- 12:00-14:00
- 14:00-18:00
- 18:00-22:00
- 22:00-07:00

- I do not use Blackboard

Q13 of 34 - For each of the statements below, choose whether you strongly agree, agree, are neutral, disagree or strongly disagree:

- Using Blackboard gives me more access to my lecturers
- Using Blackboard gives me more access to classmates
- Using Blackboard changes the hours I can study
- Using Blackboard gives me more access to resources and learning materials
- Getting notes on Blackboard makes me less likely to go to lectures
- I am more likely to communicate with my lecturer when using Blackboard (via email or the discussion board, etc.)
- Blackboard mainly repeats what is covered in class
- Blackboard adds to what is covered in class
- Blackboard helps to clarify what has been covered in class
- I would like my lecturers to make more use of Blackboard
- I would prefer getting material in hardcopy handouts to having it put on Blackboard
- Using Blackboard makes it easier for me to learn
- Using Blackboard helps me understand how well I am doing

Q14 of 34 - Are there other ways, good or bad, that using Blackboard affects your learning?

Q15 of 34 - Do you use your University email account for your correspondence with lecturers and fellow students on course-related matters?

- Always
- Sometimes - I sometimes use the university email account but also use a second email account

- Never - I never use my University email account
- Not applicable - I don't email at all.

Q16 of 34 - Can you tell us why you prefer to use this email account?

Q17 of 34 - Do you ever share files with other students on your course electronically? If so, how? (Tick all that apply)

- Using Blackboard
- Using a USB stick
- Using email
- Using Google Docs
- Using Drop.io
- Using Dropbox.com
- Using Yahoo Groups
- Using another online sharing site or social network
- I do not share files electronically with other students on my course.

Q18 of 34 - Please let us know whether you agree or disagree with the following statements:

- I would like to be able to receive Blackboard course notifications and updates on Facebook
(Select 'Not Applicable' if you do not use Facebook)
- I would like to be able to use a Blackboard App to access course notifications or updates using my iTouch/iPhone
(Select 'Not Applicable' if you do not own an iTouch or iPhone)

Q19 of 34 - What is the most important thing you would like to see improved about the Blackboard service?

- More reliable
- Easier to use
- Better usage by lecturers
- More use of multimedia resources (e.g. audio or video)
- I don't have an opinion on this

Q20 of 34 - If you could change one thing about how Blackboard operates, or how it is used by staff, what would that be?

Q21 of 34 - For each of the statements below, indicate whether you strongly agree, agree, disagree or strongly disagree:

- I am comfortable using computers
- I have adequate access to a computer and the internet outside of the university
- I think systems like Blackboard are helpful
- Blackboard is easy to use
- Blackboard is reliable
- I can get adequate help and support to use Blackboard

Q22 of 34 - Please let us know your thoughts on the following, by selecting Yes No Not Applicable:

- Have you ever taken a Multiple Choice Quiz exam through Blackboard?
- Would you like to take Multiple Choice Quiz exams through Blackboard in the future?
- Have you ever submitted assignments (essays, projects) using Blackboard?
- Would you like to submit assignments using Blackboard in the future?
- Have you ever accessed your provisional grades through Blackboard?
- Would you like to access your provisional grades through Blackboard in the future?

Q23 of 34 - Do you have any additional comments about handing in assignments (essays or projects) or completing Multiple Choice Quizzes on paper versus using Blackboard to submit online?

Q24 of 34 - Currently, each course on Blackboard is accessible only to registered students and those involved in the delivery of that course (academic staff and/or tutors). Do you agree with this policy?

- I would like only registered students to have access to my courses on Blackboard
- I would like anyone (at University) to have access to my Blackboard modules
- I would like anyone (anywhere on the internet) to have access to my Blackboard modules

Q25 of 34 - What is your gender?

- Male
- Female

Q26 of 34 - What is your age?

- 16-23
- 24-35
- 36-50
- 50+

Q27 of 34 - What field are you studying?

- Medicine/Health
- Science
- Engineering

- Arts/Humanities
- Business or Law
- Other

Q28 of 34 - What course are you studying?

Q29 of 34 - What year of your course programme are you in? And are you an Undergraduate or Postgraduate of the course?

- First year
- Second Year
- Third Year
- Fourth Year
- Fifth Year
- Longer

Q30 of 34 - How do you attend the university? And are you attending Part Time or Full Time?

- Day student
- Evening student
- Distance learning student

Q31 of 34 - Do you have a disability/learning difficulty that affects your learning experience at the university and your use of Blackboard? (Tick all that apply)

- Dyslexia
- Deaf/Hard of Hearing
- Blind/Visual Impairment
- Physical Disability
- Other Disability

- Not Applicable

Q32 of 34 - If you have a disability, how has using Blackboard affected you?

Q33 of 34 - Have you any additional comments, ideas or suggestions on the use of technology, in general, for teaching and learning at University that you wish to share?

Q34 of 34 - This survey is anonymous. However, if you would like to be included in the prize draw, please provide your University student email address. (This information is not retained).

Annotated Bibliography

Babu, Sarat Chandra. (2001). *E-Learning Standards*. Retrieved February 4, 2010, from

<http://www.cdac.in/html/pdf/Session6.1.pdf>

An overview of e-learning standards is presented. The introduction provides a brief look at e-learning including an outline of the benefits of using an e-learning solution. Some of the benefits highlighted include: increased quality and value of learning, increased flexibility and decreased cost of learning delivery.

Issues with e-learning are also presented. The issues include concerns regarding scalability, interaction, security, interoperability and inter-changeability. The evolution of e-learning standards is discussed. Each of the following standards are briefly explained, AICC, PROMETEUS, ARIADNE, Advanced Distributed Learning Initiative (ADL), Shareable Courseware Object Reference Model (SCORM).

This is followed by a detailed explanation of the standards, IMS (Instructional Management System) Global Learning Consortium and the IEEE Learning Technology Standards, including the standards and specification development organizations and the LTSA Architecture

Bevanda, Vanja., Azemović, Jasmin., Mušić, Denis. (2009). *Privacy preserving in eLearning*

environment (Case of modeling Hippocratic database structure), Fourth Balkan Conference in

Informatics. Retrieved February 4, 2010 from

<http://www.ieeexplore.ieee.org/libgate.library.nuigalway.ie/stamp/stamp.jsp?tp=&arnumber=5359353>

The development and implementation of a Hippocratic database structure within e-learning systems is presented. This process encompasses the application of W3C requirements and standards.

Hippocratic databases created from the basic principles of the Hippocratic Oath, allows for the preservation of privacy in information systems. A model for student mobility issues is also detailed, although it is contradictory to some of the Hippocratic database principles.

An outline of the role and issues of privacy, security and access control in databases systems is first presented, including examples of privacy violations. Next the Hippocratic database in an e-learning environment is explained, starting from the inspiration of the basic principles of the Hippocratic Oath to the application of these principles on a database system.

The research in this article outlines ten principles, including a detailed explanation for each. Although not yet implemented against a complete e-learning system the theory suggests that if implemented it could “prevent privacy violation and greatly simplify access control policy administration tasks”. Following this the author proceeds to demonstrate the implementation of all ten Hippocratic database principles against one section of an e-learning environment, specifically the section dealing with student personal data. It is noted that some of the principles did conflict with the e-learning functionality. The resulting model presented is a normalized relational model, with the ten principles applied. However the authors do acknowledge that to keep this proposed model functioning would prove expensive, difficult and has a high possibility of the introduction of “common mistakes”.

Borcea, Katrin., Donker, Hilko., Franz, Elke., Pfitzmann, Andreas., Wahrig, Hagen. (2006). *Towards privacy-aware eLearning, Privacy Enhancing Technologies, Vol 3856, p167-178*. Retrieved February 5, 2010, from <http://www.springerlink.com/content/9128236834464122/>

A discussion takes place as to the requirement for privacy-enhancing application design. E-learning is used as the example for the discussion. A solution is also presented which applies

privacy enhancing identity management (PIM) to ensure a higher level of anonymity to an e-learning environment while still allowing the system to assist users.

Throughout the introduction, a discussion takes place on the need for an e-learning environment to assist users in the learning process, however to achieve this, a system must ascertain information about the user. Hence data collection is necessary regarding the users profile, which in turn raises the question of security and privacy protection. This discussion leads into the next section dedicated to an overview of the principles of privacy and security. A short outline is provided of the main terms and issues relating to identity management.

Following this an introduction to e-learning is provided. This section of the article outlines the evolution of e-learning systems, from the initial sharing of video data in “Teleteaching” systems to the complex e-learning applications of today. After this introduction, a section on the privacy issues relating to e-learning is discussed. These issues are discussed by means of roles/use cases and privacy threats, resulting in requirements on PIM.

Finally a privacy enhancing solution based on PIM is presented. The overall structure is outline first followed by a detailed explanation of how the solution can be implemented.

Borcea-Pfutzmann, Katrin., Liesebach, Katja., Pfutzmann, Andreas. (2005). *Establishing a Privacy-Aware Collaborative eLearning Environment*, Proceedings of the EADTU Annual Conference 2005. Retrieved January 29, 2010 from

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.5166&rep=rep1&type=pdf>

A concept which aims to provide privacy for users while accessing a collaborative environment is presented.

The motivation for this paper discusses the concept of privacy in relation to standard e-learning. This discussion moves to explain the importance of expanding this privacy to collaborative e-

learning user identities. The author's objective is to examine the level of privacy achievable within a collaborative e-learning environment, with an ultimate goal that "such an e-learning environment would provide a clear mapping of traditional learning styles with the electronic world".

A discussion takes place on security and privacy in the e-learning world. The ELENA project is mentioned as an example of a team attempting to examine security and privacy for e-learning. However it is highlighted that the few exceptions analyzing security and privacy to date are only for non-collaborative environments.

An approach towards the design of an e-learning environment which supports user's natural behavior is presented next. Two main principles are highlighted with regard to the design process of an e-learning environment. They are (1) "The behavior of the eLearning users within the electronic environment should closely correspond to their natural behavior in the real world" and (2) "Each user should have free access to all functionalities offered by the environment".

The design of a privacy enhanced collaborative e-learning environment is also introduced. The objective of this design is to help users manage their learning processes and divide their activities in such a way that they can work collaboratively but also have the assurance of privacy protection.

Cárdenas, Roberto Gomez., Sanchez, Erika Mata. (2005). *Security Challenges of Distributed e-Learning Systems, ISSADS 2005, LNCS 3563, p538–544*. Retrieved January 25, 2010, from <http://www.springerlink.com.libgate.library.nuigalway.ie/content/42xu6r68k8thmw2y/fulltext.pdf>

The security challenges relevant to a distributed e-learning system are presented. First an outline of the security requirements for a distributed system is provided, with a specific focus on Internet environments. Examples of attacks are provided, including (1) replay attack, (2) “the man in the middle”, (3) IP spoofing, (4) hijacking, (5) denial of service. The need for security requirements to be determined by first understanding how an attack can occur is emphasized. A review of security issues with regard to the clients, servers, databases and legacy systems is also provided. The review divides into sections discussing, information access and control, security handlers and processing, and the needs of legacy components.

The e-learning domain is presented next including a discussion on emerging technology trends. The trends show that the interoperability within components, applications and systems of an e-learning domain is highly desired. However this interoperability although similar is normally produced on a per institution basis. Two main outcomes of the learning technology standardization process are also outlined. The first involves the specifications of information models and is assisted by standards such as Learning objects metadata (LOM) developed by IEEE. The second involves the definition of architectures, components and software interfaces for managing the model outline in the first outcome. The second outcome is considered to still be in its infancy. An overview of a tool called ReBol (Relative Expression-based object language) is presented. This tool is a messaging language for distributed Internet based applications.

Based on the information discussed in the article the authors present a summary of the major distributed e-learning security challenges in the final section.

Eibl, Christian Josef. (2009). *Privacy and Confidentiality in E-Learning Systems*, 2009 Fourth International Conference on Internet and Web Applications and Services, P638 - 642. Retrieved

February 11, 2010, from

<http://www.ieeexplore.ieee.org.libgate.library.nuigalway.ie/stamp/stamp.jsp?tp=&arnumber=5072591>

A security concept which also caters for the requirements provided by the learning process is investigated. This investigation also includes a discussion on conceptual problems with regard to confidentiality of personal data held within a learning management system (LMS). The article is based on requirements specified by educational science and the results obtained when these requirements are applied to e-learning systems.

First the requirements are detailed. This section is divided into (1) design criteria, which details the requirements and (2) consequences for practical systems, which maps the requirements to the e-learning systems. The requirements outlined should primarily be used to support the learning process however they do provide a guide to the limitations for practical systems. Three main consequences of applying the requirements are presented, they are (1) complexity and working definition of e-learning systems, (2) privacy related limits for security, and (3) distraction related limits for security. A case study focusing purely on the confidentiality also takes place. This includes a review of: (1) conceptual problems, such as invitation to courses, log on as a different user and communication content and (2) consequences for the LMS, such as authentication, global roles and integrated messaging.

The author concludes the article with a recommendation that although the user must have confidence in the security of a system it is equally important that the security doesn't impact negatively on the learning process.

Eibl, Christian Josef., (2008). *Risk Analysis towards Secure E-Learning, ICT and Learning for Net Generation (LYICT)*. Retrieved January 27, 2010, from

<http://cs.anu.edu.au/iojs/index.php/ifip/article/view/1016/20>

A risk analysis of mapping requirements determined by educational science to a technical implementation is performed. The analysis includes the disclosure of issues relating to the requirements and an overview of the consequences for the information security mechanisms. The objective was to implement a secure e-learning architecture which met the requirements of both the discipline of the learning process and the discipline of the informatics systems. The research methodology and related work is first outlined. Following this a detailed discussion takes place on the educational science requirements. Examples of some of the requirements are equal opportunities, priority to meet learning objectives, flexible learning and integration into the learning environment.

The next section presents the risk analysis of these requirements. This analysis is performed through the process of “Use Cases”. From each of these use cases potential problems were extracted and highlighted. Finally, information security and technical consequences of applying the requirements is presented.

Eibl, Christian J., von Solms, Basie S.H., Schubert, Sigrid. (2006). *A Framework for Evaluating the Information Security of E-Learning Systems, Information Technologies at School: P83*.

Retrieved February 4, 2010, from http://www.die.informatik.uni-siegen.de/DIE_BIB/Forschung/Publikationen/2006/ISSEP2006.pdf

The issue of information security in e-learning systems supported by information and communication technologies (ICT) is investigated. A new framework for assigning a security rating to an e-learning system is introduced.

The first section presents the motivation and research objectives behind this investigation. The author explains how susceptible an e-learning system is to information security breaches. One example used is the fact that e-learning environments are dependent on network connections to reach their users and as such are then susceptible to the security risks relating to the network. The negative impact to an institution if an e-learning systems security was breached is also discussed. The author does highlight that although the framework introduced will classify the security of the software based on its concept it will not classify the security on the implementation of the software.

The next section discusses the security pillars which will be used to create the criteria for the framework. The security aspects outlined, include, confidentiality, integrity, availability, identification, authorization, non-repudiation. The different types of e-learning systems are also reviewed. Finally an outline on how to measure security is provided.

The following sections outline the creation of the criteria catalogue based on the security pillars discussed earlier and provides a detailed explanation of the formula used to calculate the security rating for the software.

El-Khatib, Khalil., Korba, Larry., Xu, Yuefei., Yee, George. (2003). *Privacy and Security in E-Learning*, *International Journal of Distance Education Technologies* Oct-Dec2003 , Vol. 1 Issue 4, p1-19. Retrieved January 16, 2010, from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.7927&rep=rep1&type=pdf>

Privacy and security issues associated with e-learning are examined. The basic principles supporting privacy and legislation are discussed. Analysis and resulting capabilities of existing privacy aiding technologies are presented, this includes network and policy based privacy along with security management.

Privacy principles are first explained. The principles are presented in a table format and are taken from the Personal Information Protection and Electronics Document Act of Canada.

Although the complete set of ten principles is difficult to embed in any system, they do provide a way to analyze the capability of a technology to provide privacy. Later in the article the author uses another table to simplify the principles and suggests how each may be implemented into a system. Possible privacy enhance technologies for e-learning are also reviewed.

The next section of the article looks at the current e-learning standards with regard to security and privacy. Some of the standards discussed include (1) IEEE P1484, a learning technology standard prepared by the Learning Technology Standards Committee (LTSC) of IEEE Computer Society, (2) IMS Learning Information Pack (LIP), deals with the integration of learner information systems with internet learning environment supporting systems, (3) Aviation Industry CBT Committee (AICC), provides suggestions on e-learning platforms and is mainly focused on implementation aspects.

Privacy and security requirements are then outlines. First the Learning Technology System Architectural model is presented, followed by a discussion on three core requirements, Fundamental Privacy, Network Privacy, and Location Privacy.

A number of privacy enhancing technologies are examined next, each of which meets the requirements for e-learning systems. The platform for privacy preferences project developed by WWW consortium (W3C) is analyzed first. Although recognized as a positive contribution for privacy protection, it alone does not ensure strong privacy practices. Each weakness is outlined in detail. Network privacy is reviewed next and although considered an important safeguard, at this point in time it may be sufficient to offer just a secure channel for exchange of information between the e-learning system and client. Policy based approach for security/ privacy

management is also presented, including the difficulties encountered when the principle of limiting collection is introduced.

Areas such as trust mechanisms, e.g. certificate based mechanisms, and secure distributed logs are also outlined.

Franz, Elke., Borcea-Pfitzmann, Katrin. (2006). *Intra-Application Partitioning in an eLearning Environment – A Discussion of Critical Aspects, Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)*. Retrieved January 27, 2010, from <http://www.ieeexplore.ieee.org.libgate.library.nuigalway.ie/stamp/stamp.jsp?tp=&arnumber=1625399>

The preservation of privacy through the use of intra-application partitioning (IAP) is presented. Aspects which need to be considered when partitioning users personal data is discussed, including a proposal of possible solutions. This article also analyses the issues related to distance learning and shows how these issues are not exacerbated when using privacy enhanced learning system.

The introduction discusses the concept of privacy within an e learning environment and leads into an overview of the Privacy-Enhanced identity Management (PIM). The concept of Intra-Application Partitioning is presented next. This includes an outline of the critical aspects which should be taken into consideration. Some of the critical aspects discussed are, authenticity, accountability, preventing illegal access and assessment.

How to preserve privacy by using IAP is presented. First the e-learning system BluES'n is introduced. This system acts as a reference system for concepts in relation to IAP. The authors use examples to demonstrate how IAP can be applied. It is noted that each example is presented

from the user's perspective. Finally a discussion takes place regarding the critical aspects which were presented earlier in the document.

Further user acceptance testing and a recommendation for an investigation into "the reputation and awareness within a privacy-enhanced eLearning environment" are suggested.

Gong, Guo-quan., Qiang, Shuang., Wang, Jun.(2009). *Information Security Measures and Regulation Research*, 2009 International Conference on Management Science & Engineering. Retrieved

February 26, 2010 from

<http://www.ieeexplore.ieee.org.libgate.library.nuigalway.ie/stamp/stamp.jsp?tp=&arnumber=5317613>

An information security decision model is presented. The objective is that the model will aid online enterprises in deciding the optimal information security deployment to use.

Construction of the information security model is presented first. The creation of the model is explained in a mathematical context, based on probability. An analysis of the model against independent and infectious threats takes place. The definition of an independent threat is first outlined followed by a mathematical analysis. Next the infectious threat is discussed through the use of examples.

An analysis of government regulation policies including recommendations for an information security policy is provided. To perform the analysis, an assumption that government jurisdiction extends to that of enterprises within the internet and as such have the power to regulate the market and introduce an information security tax is made. This assumption enables the author to perform a mathematical analysis on the tax income under complete and incomplete information conditions.

Graf, Frank. (2002). *Providing security for eLearning, Computers & Graphics, Vol. 26 Issue 2, p355.*

Retrieved January 27, 2010, from

http://www.sciencedirect.com.libgate.library.nuigalway.ie/science?_ob=MIImg&_imagekey=B6TYG-452F8YX-1-1&_cdi=5618&_user=103680&_pii=S0097849302000626&_orig=search&_coverDate=04%2F30%2F2002&_sk=999739997&view=c&wchp=dGLbVlz-zSkzk&md5=1680148d56a67693f5b36151f4a5face&ie=/sdarticle.pdf

The security requirements of internet based learning are discussed. Two solutions are introduced. The first solution presented is a framework for secure testing, the second solution is focused on the issue of data protection with regard to confidentiality and copyright.

First a review is provided on the origins of e-learning. This then leads into a discussion on “why eLearning needs security”, which includes an outline of the value of knowledge. The next section analyses the security issues relate to e-learning. The following areas are discussed: (1) protection against manipulation, specifically from the side of the students, some solutions mentioned include, encryption, digital signatures and firewalls, (2) User authentication, reliable identification of a user is vital in securing an e learning system. Areas such as access control, billing, user profiles, certification, passwords and biometric identification are all examined. (3) Confidentiality, the protection of data distributed through an e-learning environment is reviewed, (4) Copyright protection and (5) shortcomings in the functionality of the WWW. Finally an overview of the Cryptographic Intellectual Property Rights Enforcement System (CIPRESS) is presented, including a discussion on how this system could be applied to E-Learning.

Igras, Eugene. (2003), *E-Learning Standards and Technology*, IRIS Systems, Inc. Retrieved January 21, 2010, from http://irisinc.ab.ca/WhitePapers/E-Learning_Standards_And_Technology.pdf

Learning industry standards and the main components of learning technologies are reviewed.

The review is divided into two sections. One presents the conceptual view, which describes the high level architecture involved in learning systems. The second presents the implementation-oriented view, which describes the standards and standardized architectural framework.

A brief overview of the standards is provided first. The standards discussed are, (1) the Aviation Industry CBT Committee (AICC), (2) The Instructional Management System (IMS), (3) Advanced Distance Learning Shareable Courseware Object Reference Model, (ADL SCORM) and (4) the Institute of Electrical and Electronics Engineers Learning Technology Systems Architecture (IEEE LTSA).

Next a conceptual view of the Learning Technology System Architecture (LTSA) is presented.

This architecture endorses the implementation of “components and subsystems which are reusable, cost-effective and adaptable”. An overview of learning technology is provided, which outlines the main differences between learning systems and the LTSA model. Commercial Learning Technology vendors and products are detailed next. Systems such as learning content development systems, learning management systems, and virtual classroom systems are all discussed. Finally the author presents how to select an e-learning technology. This is achieved by presenting the reader with the steps involved in the process.

Jerman-Blazic, Borka., Klobucar, Tomaz. (2005). *Privacy provision in e-learning standardized systems: status and improvements*, *Computer Standards & Interfaces Jun2005*, Vol. 27 Issue 6, p561-578. Retrieved January 29, 2010, from http://www.sciencedirect.com.libgate.library.nuigalway.ie/science?_ob=MImg&_imagekey=B6

[TYV-4DHWR31-1-](#)

[1&_cdi=5628&_user=103680&_pii=S0920548904001047&_orig=search&_coverDate=06%2F30%2F2005&_sk=999729993&view=c&wchp=dGLbVIW-zSkWb&md5=e05c148b7ffbc7e9d0ca2d0d8c9ec7ce&ie=/sdarticle.pdf](#)

An analysis of e-learning standards with a specific focus on privacy provision policies is presented.

First the elements necessary for privacy provision and data protection are discussed. A summary is presented of privacy threats which users may be exposed to. This incorporates a brief look into security failures, monitoring, data disclosure, limited control and collection of data. Requirements for privacy and data protection are reviewed with some discussion on the most relevant technologies.

Next an overview is provided of the current e-learning standards including the standards provided by IEEE's Learning Technology Standardization Committee (LTSC), the IMS Global Learning Consortium, the Aviation Industry CBT Committee (AICC), and the U.S. Department of Defence Advanced Distributed Learning (ADL).

An analysis of the privacy attributes within e-learning profile standards is presented next. Four main standards are used in this analysis. They are, (1) IEEE LTSC Personal and Private Information draft standard, (2) IMS Learner Information Package (LIP), (3) Internet2/EDUCAUSE EduPerson collection of attributes, and (4) the Universal Learning Format (ULF).

Finally a solution to the privacy protect issue within e-learning systems is introduced. This solution is in development by the ELENA project from the European IST programme.

Kambourakis, Georgios., Kontoni, Denise-Penelope N., Rouskas, Angelos., Gritzalis, Stefanos. (2004).

A PKI approach for deploying modern secure distributed e-learning and m-learning

environments, Computers & Education Jan2007, Vol. 48 Issue 1, p1-16. Retrieved February 16,

2010, from

http://www.sciencedirect.com/libgate.library.nuigalway.ie/science?_ob=MImg&_imagekey=B6

[VCJ-4FDMY9V-1-](http://www.sciencedirect.com/libgate.library.nuigalway.ie/science?_ob=MImg&_imagekey=B6)

[1&_cdi=5956&_user=103680&_pii=S0360131504001745&_orig=search&_coverDate=01%2F3](http://www.sciencedirect.com/libgate.library.nuigalway.ie/science?_ob=MImg&_imagekey=B6)

[1%2F2007&_sk=999519998&view=c&wchp=dGLbVtb-](http://www.sciencedirect.com/libgate.library.nuigalway.ie/science?_ob=MImg&_imagekey=B6)

[zSkzk&md5=c13e1e034b7e6831cce95c76391ee3bc&ie=/sdarticle.pdf](http://www.sciencedirect.com/libgate.library.nuigalway.ie/science?_ob=MImg&_imagekey=B6)

A trust model which supports the activities of both e-learning and m-learning environments is presented. The trust interactions between the learners and the e-learning providers is outlined through the demonstration of the implementation of security mechanisms and trust control.

The introduction reviews the need for trust within the learning environment, from the original face to face education up to the current usage of e-learning and m-learning environments. M-learning is defined as the use of “mobile technology in education”. The introduction continues into an explanation into the terms public key infrastructure (PKI) and attribute certificates (AC’s). Each of which plays a key role in security, in particular in the area of authorization information.

The first section outlines the trust model with particular focus on the integration of Public Key Infrastructure (PKI) into the system. Next the trust model is assessed through the use of scenarios based on learner and provider interactions. The application of attribute certificates (AC’s) to m-learning is also evaluated.

Finally, performance times are reviewed through the analyses of the trust model and application of AC's proposed solutions with regard to service response times. A test bed of mobile devices against a mobile educational system is used to retrieve the times

Mwakalinga, Jeffy., Kowalski, Stewart., Yngström, Louise. (2009). *Secure E-learning using a Holistic and Immune Security Framework, Internet Technology and Secured Transactions, ICITST 2009.*

Retrieved February 2, 2010, from

<http://www.ieeexplore.ieee.org.libgate.library.nuigalway.ie/stamp/stamp.jsp?tp=&arnumber=5402508>

How to secure an e-learning environment by using a holistic and immune security framework is presented. The application of the principles of Immune system to a secure e-learning system is explained. The insecurities created in e-learning systems by the general culture of users are also discussed.

A brief definition of e-learning is first provided followed by an explanation on the culture affects of how users interact with an e-learning system. It is deemed important that e-learning systems should be able to adapt to their operational environments and to the cultures of their specified users.

Next the developed Holistic and Immune framework is presented. This framework is based on the "Systemic-Holistic" approach and includes the principles of the immune system. The explanation of the framework includes a listing of each of the components contained within the framework and a detailed discussion on how each component works. Following this a discussion takes place on how the e-learning security system needs to be able to adapt to facilitate users of different cultures. To prove this the authors applied a number of different environment analyzers to the e-learning environments and culture of users. The analysis was

based on (1) the “Systemic-holistic” approach, (2) the “Cybernetic Structural” model and (3) the “Viable System” model.

The “E-learning System Users Cultural Values Analyzer” is discussed in detail. The authors reference a survey of three cultures experience while using an e-government site. This survey showed that users of different cultures encounter different issue while using the site. This logic was then applied by the authors to develop an e-learning user’s values analyzer which examined the effects of a user’s culture, laws and traditions on the security of an e-learning system. From this an informal culture model was formed which can predict an e-learning systems behavior based on the users culture. The author concludes the article, with an admission that the security framework has only been tested on a limited basis and in fact has yet to be fully implemented. Future research work will focus on a full implementation and performance monitoring of the framework.

Stapić, Zlatko., Orehovački, Tihomir., Danić, Mario.(2008). *Determination of optimal security settings for LMS Moodle, MIPRO 2008 - 31st International Convention on Information and Communication Technology, Electronics and Microelectronics*. Retrieved January 15, 2010, from <http://crosbi.znanstvenici.hr/prikazi-rad?lang=EN&rad=357101>

Optimal settings for a Moodle server to prevent specified security issues are presented.

Recognition is given to the need for security measures to exist on the server and not be solely dependent on the security measures provided by the Moodle application. The evolution of the virtual learning environment (VLE) is first reviewed. The origin of the VLE begins in the 1960’s at the University of Illinois with a system called “Plato”, which continued to thrive until 2006. The next breakthrough in the evolution was in 1997 with WEBCT 1.0 and Blackboard emerging onto the market. Moodle followed in 1998. The paper is divided into three main

sections, starting with a focus on the security and privacy vulnerabilities, including a review of threats to a Learning Management System (LMS) regardless of the vendor. These threats are divided into four groups, authentication, availability, confidentiality and integrity attacks, each of which is explained in detail. An overview of the Moodle architecture including a discussion on possible weaknesses from a security point of view is then presented. Only the second layer of the Moodle multi layer architecture is discussed, the paper does not discuss security vulnerabilities at the database or client layers. The final section details recommended security settings based stress test results performed against the authors Moodle install.

Tsiantis, L. E., Stergiou, E., Margariti, S. V. (2007). *Security Issues in E-learning Systems*, AIP Conference Proceedings, Vol. 963, Issue 2, p959. Retrieved February 4, 2010, from http://content.ebscohost.com/pdf19_22/pdf/2007/86P/26Dec07/28153993.pdf?T=P&P=AN&K=28153993&EbscoContent=dGJyMNxb4kSeprE4y9fwOLCmr0iep7JSsqy4SLeWxWXS&ContentCustomer=dGJyMPGsr0%2BwqbFIuePfgeyx%2BEu3q64A&D=aph

The development of security mechanisms which takes into consideration the users is proposed. The introduction provides a discussion on the importance of security and the unfortunate side affect of some security mechanisms on the usability of the system. In particular authentication and privacy issues with regard to usability of online learning environments are outlined. The author proposes that the technical mechanisms used to secure a system do not “fit well” with a learning environment. The concept of a learning environment is such that it is dependent on a “tradition of trust, information exchange and discussion”, while the security domain is built on a “culture of distrust, restricted information flow and autocratic rules”. Two aspects of security are however highlighted. They are confidentiality, involved in the protection of information and integrity, involved in maintaining the condition of the data.

Next a discussion takes place with regard to authentication and the role it plays in ensuring confidentiality and integrity are maintained. Authentication is divided into two stages. First the identification of the user by means of a unique id and the second the verification of the user by the means of a secure password. Three ways in which a user can authenticate are presented.

They are (1) Knowledge based, (2) token based, and (3) biometrics. As knowledge based authentication is the most commonly used form, the discussion moves on to review passwords. How to create a secure password is outlined, including recommendations on the length of the password, character sets used and lifetime of a password are all discussed in detail.

The following section analyses the role of privacy in management of data. The value of ownership with regard to data and how this can be translated into the determination of access rights are discussed. Finally an explanation of LDAP authentication takes place. This includes an overview of the tree structure used in LDAP directories and the password file.

Varlamis, Iraklis., Apostolakis, Ioannis. (2006). *The Present and Future of Standards for E-Learning Technologies, Interdisciplinary Journal of Knowledge and Learning Objects Volume 2.*

Retrieved January 12, 2010, from

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.9621&rep=rep1&type=pdf>

E-learning technologies are examined from the point of view of standardization. A detailed review of the existing standards is provided, including an overview of the e-learning lifecycle and infrastructure. A software and hardware independent e-learning model is presented. A framework for developing a global e-learning standard which is capable of supporting interoperability of e-learning systems is defined.

The introduction starts the discussion of the need for standardization of e-learning. How the standards are developed is outlined, including the lack of interoperability within the standards. Some of the goals of e-learning are presented with a view that if standards were defined and adopted completely would result in the goals being achievable. The goals listed include the ability to move between programs and platforms by the user, the standardization of learning content format and the decrease in cost to develop tools used by e-learning platforms.

Next, a detailed look at the inside of the e-learning process is presented. This begins with an overview of the lifecycle of the e-learning process, starting with the course planning and ending with the assessment of a learner's knowledge following completion of the course. The lifecycle provides a visual on the issues of interoperability and standardization of tasks within the e-learning process, each of which are discussed.

The e-learning systems infrastructure is presented next. Infrastructure in this discussion is the "elementary particles of an e-learning system known as learning objects." Learning objects are defined in the article as "chunks of data used by the e-learning system".

E-learning Standards are presented in detail. The merits of standardized technologies are listed as Interoperability, Re-usability, Manageability, Accessibility, Durability and Scalability, each of which is briefly explained. Next the four steps involved in creating e-learning standards are presented. They are specification, validation, standardization and dissemination.

Finally Interoperability of E-Learning Technologies is discussed. Some of the issues related to interoperability of e-learning tools are also presented in detail. They are metadata, packaging, learner management and communication.

Yong, Jianming. (2007) *Security modeling for e-learning, Proceedings of the 2007 IST International Symposium on Information Technologies and Applications in Education (ISITAE 2007)*.

Retrieved February 18, 2010, from

<http://www.ieeexplore.ieee.org.libgate.library.nuigalway.ie/stamp/stamp.jsp?tp=&arnumber=4409226>

An analysis of the challenge of providing security within e-learning is presented. An overview of the four main e-learning organizations, namely, Aviation Industry Computer based training committee (AICC), IEEE Learning Technology Standards Committee (LTSC), Instructional Management Systems (IMS) Global Consortium and Advanced Distributed Learning (ADL), is provided. The main objective of the paper is to attempt to address the right access control mechanism for e-learning. The first section of the paper, reviews the authors contribution to date to the extended RBAC (ERBAC). This is followed by a detailed discussion on specific roles and attributes relevant to e-learning. Finally the last section presents the architecture of security modeling for an e-learning system. This paper focuses more on the roles and associated attributes required for each stakeholder and user involved with the e-learning system. The author recognizes that this paper is just an initial step into the analysis of roles and recommends further research in the area, specifically in the area of mapping the roles to the e-learning standards.