Summer 8-15-2017

A Security and Privacy Framework for e-Learning

Radwan Ali
Kennesaw State University, rali@kennesaw.edu

Humayun Zafar
Kennesaw State University, hzafar@kennesaw.edu

A Security and Privacy Framework for e-Learning

Radwan Ali
Kennesaw State University

Humayun Zafar
Kennesaw State University

Abstract

Prior research in the e-learning area has appeared with a focus on its adoption aspects. Limited research has been carried out solely on the interplay between e-learning and security and privacy. Considering the wide acceptance of e-learning, and a plethora of cybersecurity breach incidents, it is surprising that the two topics have not been discussed together. An effective e-learning environment depends on stakeholders who understand the importance of security and behave responsibly within it. In this paper, we present a conceptual model that looks at some of the information security and privacy factors related to e-learning.

1. Introduction

These guidelines include complete descriptions of the fonts, spacing, and related information for producing your proceedings manuscripts. Please follow them.

The playing field has been changing for higher education [11]. Multiple economic downturns have presented new financial challenges. As a consequence, colleges and universities around the United States have altered their approaches and have sought new sources of monetary support. With so many technological advances, today's web-based educational offerings represent a solid indication of new effective approaches in higher education [8]; [11]. 90% (393 out of 436) business schools accredited by the AACSB offer online courses [8].

With this evolvement and new approach to its mission, e-learning in higher education has brought with it new demands in relevance to institutional preparation **[44; 67]**, infrastructure [9], logistics and policies, and information use [17], and security risks [19]. Considering the wide acceptance of distance education, adoption of learning management systems, and a plethora of cybersecurity breach incidents, it is surprising that the two topics have not been appropriately discussed together. Graf **[31]** cited loss of confidentiality and availability, the exposure of critical data, and vandalism of public information services as security risks associated with e-learning. It is also important to note that learning management systems themselves have been a target of a cyber-attack **[45].** This issue is compounded by the fact that in many ways e-learning technologies such as learning management systems are consumer oriented, but their protection mechanisms focus on the organizational end, which is not necessarily consumer oriented. For example, organizations protect their learning resources through firewalls and anti-malware software **[75]**. However, most e-learning security issues have been attributed to a user's poor knowledge of security measures, and lack of education. This has resulted in issues such as information manipulation by outsiders and insiders, and loss of confidentiality [25]. For meaningful research to be undertaken in an arena that has a disparate set of cyber threats coupled with implementation of e-learning technologies that focus on flexibility and attainability of education there is a need for a framework that is able to coalesce this issue. After all, protecting private information (e.g. education records) can also impact an e-learner's willingness to accept e-learning **[53]**. In this study we present a conceptual model that looks at some of the information security and privacy factors related to e-learning. We base our model on previous work by Clark, Beebe, Williams, & Shepherd [16]. Previous research used other model to produce some e-learning conceptual models **[34]**, **[59], [54].** In the next few sections we provide some ancillary work that has been done in information security and the proposed conceptual model.

2. Literature Review

There is no shortage of information security models. From role based access control **[65]** to introduction of counter-measures [21], previous research has presented the security and privacy phenomenon in varying contexts. Prior research in this area has appeared sporadically under the guise of e-learning, with an evolved focus on the technical aspects of security [6; **27; 48]** . Generic frameworks have also been presented without being applied to the IS domain [29; **32]**. Some researchers have focused on the overall e-learning environment, alluding to its inherent insecure nature **[28], [56], [67], [78].** In particular, [3] presented an e-learning model that included five constructs: IT infrastructure services, perceived usefulness, user satisfaction, customer value, and organizational value. Their work was based on the premise that "…little attention has been paid to the role of IT infrastructure services in e-learning…" (p. 434). They used a study of academic staff and

students that looked at factors that influence e-learning success. Both groups separately cited security as an important aspect of perceived usefulness and user satisfaction.

A common approach taken in IS literature in modeling acceptance and use of any technology in general is the implementation of the technology acceptance model (TAM) [22]. Other technology adoption theories used include Innovation Diffusion Theory (IDT), the Unified Theory of Acceptance and Use of Technology (UTAUT), and the DeLone and McLean's (D&M) model. Some of these studies have looked into what enhances or prohibits e-learning adoption [14], [61]. In addition, Ozkan and Koseler (2009) proposed a six-dimension (hexagonal) e-learning assessment model with the acronym (HELAM). These various mentioned works have all proposed some models for e-learning that were not based on TAM.

TAM was adopted from the theory of reasoned action (TRA) [5]. One of the reasons TAM is widely used is due to its capacity to overcome the problem of underutilized systems. However, e-learning in the context of dynamic learning management systems is relatively new, and e-learners are a specific user group. Therefore, when investigating the interplay of security with e-learning, TAM alone cannot fully reflect the requirements of such a model, and that a more holistic model is needed [15]. That may also be a reason as to why limited works have applied an integrated model of IS success model and TAM to explore e-learning usage drivers **[51]**. Most research has continued to focus on adoption of e-learning instead **[47]; [53]**; [62], [63], [64] as opposed to security.

Since privacy and security can be considered as features of a e-learning platform, it is interesting to note that previous research has focused on this aspect in the context of e-commerce **[28]**, **[68]**. Some research has also rightly pointed out the important role e-learning plays in the context of employee training in non-academic settings, and how privacy and security principles need to be adequately addressed from an overarching policy and standards point of view [26]. The e-learner perspective is an important one to focus on. Raitman et al. **[56]** showed the value and benefits of fostering a sense of security in the online e-learning environment. They conducted a study that investigated student attitudes toward a wiki environment that had a user login requirement as part of the authentication process. Kumar, Gankotiya, and Dutta **[42]** presented a more comprehensive view of authentication requirements by incorporating factors such as Single Sign On (SSO), Lightweight Directory Access Protocol (LDAP), Network News Transfer Protocol (NNTP), and databases. These technologies are somewhat reflective of the evolution of e-learning technologies in an era of cloud computing. Al-Zoube, El-Seoud, and Wyne [7] put forth a high-level view of how cloud computing can be helpful in building the next generation of platform-independent tools, with scalable e-learning systems. Limited research in this area has also focused on understanding the role cloud computing systems services play in attracting students **[69]**. However, Shiau and Chau **[69]** did not look at this issue through the lens of security and privacy. Rani et al. **[61]** looked at security and privacy as one of the secondary constructs and found that both contribute to satisfaction of e-learning systems.

Based on the research mentioned, it is obvious that research in the area of security and privacy has been relegated to an individual construct that is a part of an overall acceptance model. We contend that information security is a combination of technical and behavioral factors. As technology becomes more pervasive, there will continue to be a blurring of the lines between these two factors. Therefore, it is essential for us to use a framework that considers both factors.

3. Proposed Conceptual Model

We modify a conceptual model for creating security subsystems previously introduced by Clark et al. [16]. Though this model did not focus on e-learning issues, it can be extended to it. Such approach is not new. For example, Hassanzadeh et al. **[34]** used the D&M model of information systems success to generate their own model to assess e-learning systems success. Similarly, Rjaibi et al. **[59]** proposed another model based on multiple previous works of used Alwi and Fan [4], Nickolova and Nickolov **[52],** The reason for that is that the model mirrors the National Institute for Standards and Technology's (NIST's) system development lifecycle model (SDLC). The purpose of all NIST models is to ensure that they are generic enough to be extended to different areas **[39]**. The modified model is presented in Figure 1. A brief description of each factor along with individual propositions that set the stage for future research are presented next.

3.1. Data Evaluation

The use of data in organizations usually follows certain guidelines that may reflect consistent procedures and practices of the IT team, especially the database administrator (DBA). Organizational DBMS hold data for thousands of users and these data fall into different forms. As universally understood, the integrity of data (completeness and correctness) is essential to building a robust useful database. Consequently, the security of these data should always be considered a part of its integrity.

We believe that an institution that offers e-learning programs must adopt robust measures to protect restricted, confidential or sensitive participants' data against loss or improper use by unauthorized internal

or external parties. A data management policy can help in this regard. That policy should articulate procedures and practices for data protection.

One assumes that the DBA and the database team follow universally-effective practices for data design and management.

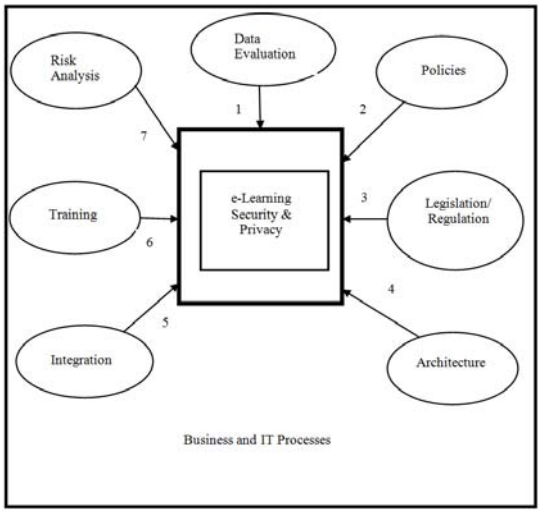

Figure 1. Factors that contribute toward Security and Privacy of e-Learning

But there is a possibility that the database-specialized team may not know what data to include fully [38]. And more, the DBA may not attribute data security measures to be security of data. Involving others around the institution may facilitate the approach to a comprehensive effective policy. Therefore we posit

P1: A full data evaluation based on the participation of all stakeholders will enhance security and privacy of e-learning technologies.

3.2. Policies

We work on the premise that organizations continue to seek improvements and all their activities are designed to help achieve these improvements. Accordingly, policies are created, refined, and implemented to help attain organizational strategic goals. When policies are initiated and adopted, the security and privacy of the stakeholders must be addressed in these policies.

While developing security policies for e-learning, many factors should be considered: 1) the student's home environment, 2) the student's use of the technology, and 3) the teacher/facilitator of the interaction. For educational institutions, their practice of using technology should be clearly stated as a measure of protection for the wellbeing of the participating student. Additionally, the integrity of the experience (plagiarism/cheating), the wellbeing of the institution (legal obligations), and the instructor's use of material (copyrights) should be included in these policies [44].

The increase of using the Internet technologies for distance teaching and learning, faculty and students have [62] must be considered also in setting these institutional policies. In addition, privacy must be treated as a strategic policy item from the various higher education stakeholders [19]. Therefore, we posit:

P2: Robust and wholesome institutional security policies that emphasize the privacy and protection of the participating students will enhance security and privacy of e-learning technologies.

3.3. Legislation/Regulation

Most organizations try to implement relatively good security plans, protections, and response capabilities. However to plan for the future, even a well-prepared entity needs to understand the driving forces that will require it to change its security planning, protections, and response. Compliance and regulations are probably the most important set of driving forces for organizations today. To be in compliance organizations invariably need to substantially improve their security. This is especially true in the areas of documentation and identity management [55]. Examples of laws include data breach notifications requirements such as California's SB 1386. Some deal with privacy protection, e.g. the European Union (EU) Data Protection Directive of 2002, and the US Gramm-Leach-Bliley Act (GLBA).

Universities are faced with compliance not just due to federal (e.g. Federal Requirement 4.8) regulations, but also under guidelines laid down by accreditation agencies such as the Southern Association of Colleges and Schools (SACS). SACS expects that each institution documents procedures that assure that security of personal information is protected in the conduct of assessments and evaluations and in the dissemination of results. Institutions are also required to have a written procedure for protecting privacy of students enrolled in distance and correspondence education courses or programs. Therefore, we posit:

P3: Comprehensive implementation of regulations will enhance security and privacy of e-learning technologies.

3.4. Architecture

This can be an overwhelming challenge for e-learning. The nature of online course delivery prompts many areas for concern with respect to security. The infrastructure of the institution and architecture of security should be designed to address the following:

• Defining user roles (students and instructors) and their identity and login [72];

• Course content and user manipulation (content addition, modification, deletion, and use) ability; and
• Access channels.As a part of the online course delivery, using a learning management system (LMS) has become common and frequent.

Many of these will be addressed via agreements (or understanding) of what the institutions will provide and what the instructor's obligations will be. For example, it is commonly understood that the instructor will be the designer/manager of the course. He/she will be the only one who can add, modify, or delete content. In the student role, the participating audience will have access based on what the instructor allows them to do using the different features in the LMS. Defining the parameters for secure access and protection of intellectual property must be addressed in the architecture. Therefore, we posit:

P4: Well-designed security architecture will enhance security and privacy of e-learning technologies.

3.5. Integration

The wide array of enterprise systems in the market poses a challenge organization with respect to legacy and current existing systems. It is assumed that if an organization were to mix and match systems, these systems must integrate well to serve the different functions of the organization. For an academic institution that offers e-learning courses, the same holds true. The LMS and its security features must mesh well with that institution's current security plan and standards.

The importance of information systems integration lies with the control and flexibility that integration affords the organization [13]. With today's technological affordances, different DL stakeholders can benefit from IS integration as it presents a complete approach to the learning experience **[72]**.

Today's organizations started to notice the need for systems that support their rapidly changing environments **[41]** Academic institutions are learning new approaches to managing themselves like business entities. Because of so many surrounding conditions, higher education is changing into different business models. The new business model includes investments in DL. That allows for new funding resources to accommodate the shrinking public resources. How is information systems integration relevant here? As tertiary institutions adapt, information technology tools will be needed to support the changing environment with respect to needs and infrastructure. In the previous section we presented architecture as an essential driver for security in DL. The architecture of information systems almost always includes integration. Therefore we posit:

P5: A complete and correct integration of information systems will enhance security and privacy of e-learning technologies.

3.6. Training

Most directives pertaining to security and privacy are captured in the security policy, and the standards. However, they will not be effective if no one knows about them and how an organization expects them to be implemented. For security to be effective, everyone from senior management on down to the rest of the staff must be fully aware of the importance of enterprise and information security **[72]**.

A security-awareness program is geared toward an individual audience to ensure that each group understands its particular responsibilities, liabilities, and expectations. Security training should happen periodically and continually. Various methods should be employed to reinforce the concepts of security awareness. Things like banners, employee handbooks, and even posters can be used as ways to remind university employees and students about their duties and the necessities of good security practices. At this juncture based on our research, training pertaining to e-learning courses is relegated to effective teaching of a distance course. It does not directly relate to security awareness **[50]**. For example, SACS questions each institution's ability to make training in technology available to faculty members teaching distance education courses. As universities continue to evolve toward hybrid and pure online teaching environments, security and privacy issues will need to be communicated and assessed. Therefore, we posit:

P6: Security training, education, and awareness programs will enhance security and privacy of e-learning technologies.

3.7. Risk Analysis

An effective risk analysis should integrate the security program objectives with a university's business objectives and requirements. The more the university and security objectives are in alignment, the more successful the two will be. The analysis will help a university draft a proper budget for a security program and its constituent security components. Once an organization knows how much its assets are worth and the possible threats they are exposed to, it can make intelligent decisions about how much money to spend protecting those assets **[77]**. SACS guidelines state that an institution has an ethical responsibility to take reasonable steps to provide a healthy, safe, and secure environment for all campus constituents, as it will contribute toward more effective risk management. Risk management/analysis according to SACS can be carried out through review of an institution's safety plan, crisis communications plan, and other health and safety procedures. However, once again, in the e-learning technology realm, specifics are lacking in terms of required guidelines. Therefore, we posit

P7: Comprehensive risk analysis will enhance security and privacy of e-learning technologies.

4. Discussion

It is undeniable that distance education has become an essential part of higher education [8]; [9]; [19]. Even at the level of middle and high school, there is a push to implement such approach. For the success of this relatively new educational approach, there are many factors to be considered. In the previous section we used the Clark et al. [16] model to put forth an argument for integrating security as an essential aspect of distance education framework. We worked on the premise that because DL has become a fixture in all levels of education, it is important that it functions within borders that assure a high level of quality **[74]**. The framework included data evaluation, policies, legislations/regulations, architecture, integration, training, and risk analysis.

A fundamental definition of an information system in relevant textbook literature (multiple references) associate five components: software, hardware, data, people, and procedures. The various components provide a holistic approach to development of robust business systems. The discussion within this document relies on the premise that information privacy and security span all of the five components. Thus, we adopted the Clark et al.'s [16] model because of its wholesome premise to protect the organization's various aspects. Said model diligently seeks the integration of privacy and security as fundamental feature into each of the five components **[41]**. The seven pillars aim to encompass and relay the essential importance of privacy and security in any information system. They acknowledge that their model has intentional redundancy because *"…one's view of a component differs when considering how it relates to the business process, security governance, and/or privacy governance subsystems…."* (p. 4)

Each of the factors mentioned above entails multiple sub-tasks. These, in turn, require some attention prior to and during implementation. Clark et al. [16] contended that security should be a fixture in systems design and not an "afterthought." This section discusses how the various factors can be treated within the context of distance education.

With the increase of human presence -- personal and professional-- online, there are calls for more security measures **[70], [46], [35].** Assumingly, sharing information online occurs within friendly confines such as a classroom. In order to protect those confines, higher education institution must consider the business relationship among a distance education set of stakeholders (students, teachers, technical staff, and administrators). Rhee et al. **[58]** discussed social distance as a construct for connectivity in a business relationship or partnership. In their study of MIS Executive, they concluded that "…firms need more security awareness training and systematic treatments of security threats instead of relying on ad hoc approach to security measure implementation" (p. 221). They added that in order for information security measures to be effective, they must address technical and human elements.

As this research adopts the Clark et al.'s [16] model as a framework for security in e-learning, we see several applications that can help address security and privacy in that environment. Table – 1 below takes the seven criteria from that model and shares potential challenges and recommends possible solutions. We expand on the literature in support of these items after the table.

In general, there are multiple risks associated with the Internet and its technologies. E-Learning has it large shares of these. The literature [4], [**52], [40],** agrees on the widespread of threats in online environment. This starts with regulating the accessibility to resources including the login process as a first step. Being a challenge, having authentication process in place is essential **[66]**. One of the best measures is to have an access log **[37]** that track users' entry and exit of the e-learning system.

Another important challenge in this case is Denial of Service (DoS) attacks. These are malicious automated robo-broadcasts that target one servers and look like calls for information. These get the server so busy that it cannot reply to legitimate workstation requests. In addition, to DoS attacks, unauthorized entry [4] and cookies [19] are other risks that require fundamental cure. Saxena **[66]** suggested a single sign-on authentication to access all course's Web resources. Such measure will provide convenience and ease to the e-learning participants in addition to ease of maintenance by the technical staff that administers the network.

Masud and Huang **[49]** argued that having a policy about using the organizational network (including the e-learning portal) would improve the users' behavior with respect to security.

Table 1 – Factors and Recommendations for Distance Learning Security

Factor	Challenges	Recommendations for e-Learning
Risk Analysis	• Denial of Service (Dos) attacks **[52]** • Unauthorized entry [4]	• A single sign-on authentication to access

	• Cookies [19]	all course's Web resources **[66]** • A policy about Web use **[49]**
Data Evaluation	• Login • Course content **[80]; [54]**	• Trust Certificates [2] • Use of biometrics/DRM **[48]**
Policies	• Human behavior **[33]** • Software/ Hardware (Czerniewics-Brown, 2009) • Roles/responsibilities **[19]**	• Establish institutional dimensions (for each policy list **[37]**
Legislations/Regulations	• Regular integration of state and national legislations **[21]** • Awareness of University system regulations/procedures **[63]** • Copyrights **[80]**	• Extending the control of the copyright holder on the entire lifetime of the digital data **[31]**. • Digital identity design and privacy preservation. **[76]**
Architecture	• Data transmission channels **[80]** • Access controls [4] • Software **[36]**	• Virtualization (Masud & Huang, 2012) • Encrypted SSL channels through the web administration interface [18]
Integration	• Student needs • Staff/Faculty Coordination **[33]** • Levels of protection	• Activity monitoring **[48]** • Exam protection **[48]**
Training	• Resources [1] • Quality **[21]**	• Readiness Measures **[37]** • Interactive instructional materials **[54]**

Selim **[67]** used a study to identify success factors (CSF) for e-learning. The study highlighted eight factors that included control for technology and attitude of teachers, student competency and attitude, and campus technology infrastructure. One of the categories was student-related. The study relayed that if students were engaged in the e-learning experience, they would account for behavior toward protection of information.

To help that accountability, an institution that commits to e-learning can put in place measures to evaluate user behavior. That includes login monitoring with respect to location, frequency, documents accessed, and other aspects.

These can be seen in infrastructure (network, hardware, and software) **[54].** As a starting point, a thorough assessment of potential vulnerabilities of e-learning system is an important step **[79]**. This assessment should entail identifying the challenges with each aspect of the Clark et al.'s model, and hence, generate a treatment or protection plan.

With each of the stakeholders lies a set of these potential threats. For example, a system administrator needs to ensure that participating students have access. In addition, the administrator handles faculty accounts and instructional designers who assist the respective faculty. In the case of the student, it is possible that he/she might share login credentials with friends or family members. As for a faculty member, he/she may share similar credentials with a graduate assistant (GRA) or teaching assistant (TA). These are just two examples of possible risks. We suggest that these risks be identified for each of the stakeholders. That will make finding treatments a more focused process. Custer [20] suggested that organizations build their own lists of vulnerabilities and benchmark them with existing national lists such as the National Vulnerability Database (NVD) produced by National Institute of Standards and Technology (NIST). He reasoned that such benchmarking would help by expediting the automation of security measures implementation. Other compliance standards can be obtained from the National Cyber Security

Division/US-CERT at the Department of Homeland Security (DHS).

Based on said analysis, relevant policies can be generated to help the respective institution proceed. These policies are documents that should convey a wholesome look into implementing the distance education program all its aspects **[33]; [21].** These policies must include information about related national and local legislation in addition to any state and university systems mandates. For example, it is important for faculty and students to know about copyrights with respect to using Web-based materials. Hence, it is safe to assume that the respective university would ensure that its policies are based on legal information received from related national, local, and institutional entities. Salmon [54] emphasize the responsibility of the faculty and staff of understanding the security policies. These documents will include guidelines for user conduct for administrators, students, faculty, and staff. Some others might include training materials and tutorials. These policies aim to shelter people and protect information as they include guidelines for behavior and details about risks and compliance [36]. Other documents might include an inventory of available resources such as hardware, software, and a blueprint of the technical architecture.

The notion of a security blueprint has to do with documenting the physical structure and its access logistics. This is a key element in ensuring that this suggested e-learning security is vigorous. Clark et al [16] reasoned that inconsistent security controls are a major risk. They added that disaster recovery plans and environmental protection procedures belong in this type of architecture. The blueprint can be greatly beneficial in coordinating the efforts of the technical staff such as the student system administrators and the institutional security team because it will define roles and responsibilities. Furthermore, the suggested architecture blueprint can serve as a launching pad for system integration. Culnan and Carlin [19] suggest "…a cross-functional privacy task force of key stakeholders can shape policy related to the privacy implications of new technologies…" (p. 13). Using automation and available tools can help audit information practices across the institution including e-learning offerings. They added that as these higher education institutions have policies for their finances and administration, they must include policies for information privacy and security.

E-learning relies on many different entities within the institution including the administration, technical staff, instructional designers, faculty, and students. The idea is to create a knowledge-sharing platform for the whole organization. Holsapple and Lee-Post **[37]** introduced an e-Learning Success model that presented solution for system design, delivery, and outcomes. The research project realized four challenges: 1) user/student attitudes; 2) the promise of the Internet capabilities has not been realized; 3) lack of a wholesome solution, and 4) the doubt in e-learning's staying power. Based on this argument, the adoption of the Clark et al.'s model can be attest to investigate at the various psychological and technical concerns of this model.

This platform can serve as a basis for an effective information security strategy. Such strategy should be tied to the whole organizational strategy as it will serve to protect the organization and ensure business continuity **[60]**. Accordingly, the stakeholders will have their own sets of needs and resources. With effective integration resources are channeled toward satisfying the needs, and consequently, providing a healthy e-learning environment that can help participating students succeed.

The student is an essential component to the success of the proposed framework. From that perspective, students can provide a helpful perspective that may positively affect the framework as they share attitudes and suggestions for the various component and potential implementation plans. Zhao et al. **[79]** emphasized the demand of the shift from the traditional campus to e-learning programs. They discussed planning and development of an infrastructure to minimize challenges and pitfalls. They attributed the readiness of faculty and students to be a big piece of the undertaking.

5. Implications, Future Research, and Conclusion

This research used a known security and privacy model [16] and extended it to e-learning based on previous practices of similar modes. E-Learning has become a fixture in higher education and therefore, its security becomes an important matter that should be properly treated. We conveyed that a wholesome risk analysis should be conducted to identify vulnerabilities and challenges. Accordingly, based on the findings, policies and procedures are charted to ensure compliance. In addition, an assessment of resources and training needs will be necessary as well. Accordingly, educating and preparing the stakeholders to counter these risks will become easier.

An effective e-learning environment depends on stakeholders who understand the importance of security and behave responsibly within it. One piece of the responsibility is to ensure that the various stakeholder entities are well trained [16]. After an organization makes commitment to e-learning, it is important that the organization envisage the initiative as an important piece of its complex system and strategy [1]. Reece and Stahl **[57]** stressed the important role of security training in developing ethical behavior and self-sufficiency in the stakeholders. They added that training carried with it an expertise distinction, in addition, to ability and dedication to the mission. An educational institution

that chooses to venture into implementing e-learning programs must complete a full analysis of its strategy, infrastructure, policies, and logistics with respect to security of those programs.

Clark et al. [16] credited Rechtin's (1991) systemic approach as a basis to their model. They listed three guiding principles: 1) aggregate closely related functions, 2) partition the model into subsystems, and 3) integrate the subsystems into a functioning system. They emphasized their rationale was also supported by Kruchten et al.'s (2006) work on software architecture. Said work produced, what later became revered, a roadmap for sound software development that stressed software architecture as a separated discipline.

Many of Clark et al.'s model areas of emphasis and its innovative paradigm lent itself to our project based on the following factors:

- Its systematic nature resonates with the structure nature of e-learning design;
- The integration emphasis in the model aligns with the need to a security framework that needs to become seamless in the emerging online classroom [4];
- The model represents a new methodology that includes strategies the are proving essential to today's organizations **[33]**;
- The organizational focus of the model lies parallel to e-learning as a social process [18]; and
- Clark et al. [16] envelope their model as an essential organizational knowledge base which is consistent with e-Learning systems distributed nature that centers on access and exchange of information **[52].**

For future research, it is important that this model be implemented and tested if interested institutions or stakeholders might explore the attitudes of the security personnel regarding the value of the proposed framework. In addition, it would be beneficial if implementation strategies are investigated.

6. References

[1] Alexander, S. (2001). E-learning developments and experiences. Education + Training, 43 (4/5), 240–248.

[2] Alhamad, M.; Dillon, T.; Chang, E. (2011). A Trust-Evaluation Metric for Cloud applications. International Journal of Machine Learning and Computing, 4(1), 416-432.

[3] Alsabawy, A. Y.; Cater-Steel, A.; & Soar, J. (2013) IT infrastructure services as a requirement for e-learning system success. Computers and Education, 69, 431-451.

[4] Alwi, N. H. M.; & Fan, I. S. (2010). E-learning and information security management. International Journal of Digital Society, 1 (2), 148-156.

[5] Ajzen, I., & Fishbein, M. (1975). Belief, attitude, intention and behavior: An introduction to theory and research: Reading, MA: Addison-Wesley.

[6] Aktan, B., Bohus, C. A., Crowl, L. A., & Shor, M. H. (1996). E-learning applied to control engineering laboratories. Education, IEEE Transactions on, 39(3), 320-326.

[7] Al-Zoube, M., El-Seoud, S. A., & Wyne, M. F. (2010). Cloud computing based e-learning system. International Journal of Distance Education Technologies, 8(2), 58-71.

[8] Baggaley, J. (2008). Where did distance education go wrong? Distance Education, 29(1), 39–51.

[9] Bailie, J. L.; Jortberg, M. A. (2009). Online Learner Authentication: Verifying the Identity of Online Users. MERLOT Journal of Online Learning and Teaching, 5(2).

[10] Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. Journal of Strategic Information Systems, 11(3), 245-270.

[11] Boubsil, O.; Carabajal, K. (2009). Implications of Globalization for Distance Education in the United States. The American Journal of Distance Education, 25(5), 699 -712.

[12] Cavusoglu, H.; Mishra, B.; & Raghunathan, S. (2004). A model for evaluating IT security investments. Communications of the ACM, 47(7), 87-92.

[13] Chapman, C. S.; Kihn, L. (2009). Information system integration, enabling control and performance. Accounting, Organizations and Society, 34, 151–169.

[14] Chen, H.-R., & Tseng, H.-F. (2012). Factors that influence acceptance of web-based e-learning systems for the in-service education of junior high school teachers in Taiwan. Evaluation and program planning, 35(3), 398-406.

[15] Cheung, R., & Vogel, D. (2013). Predicting user acceptance of collaborative technologies: An extension of the technology acceptance model

for e-learning. Computers & Education, 63, 160-175.

[16] Clark, J.G., Beebe, N.L., Williams, K. and Shepherd, L. (2009). Security and Privacy Governance: Criteria for Systems Design. Journal of Information Privacy and Security, 5(4), 3-30.

[17] Conway-Klaassen, J. M. Keil, D. E. (2010). Discouraging Academic Dishonesty in Online Courses. Clinical Laboratory Science, 23(4), 194-200.

[18] Costinela-Luminita, C. D., & Nicoleta-Magdalena, C. I. (2012). E-learning security vulnerabilities. Procedia-Social and Behavioral Sciences, 46, 2297-2301.

[19] Culnan, M. J.; Carlin, T. J. (2009). Online Privacy Practices in Higher Education: Making the Grade?. Communication of the ACM, 52 (2), 126-130.

[20] Custer, W.L. (2010). Information security issues in higher education and institutional research. New Directions for Institutional Research, 146, 23-49.

[21] Czerniewicz, L.; & Brown, C. (2009). A study of the relationship between institutional policy, organizational culture and e-learning use in four South African universities Computers & Education, 53, 121–131

[22] D'Arcy, J., Hovav, A. and Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research, 20 (1), 79-98.

[23] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 319-340.

[24] De Clercq, J. (2002). Single Sign-On Architectures. Published in InfraSec 2002 Proceedings, Bristol, UK, October 1-3, 40-58.

[25] De Freitas, S. Oliver, M. (2005) Does E-learning Policy Drive Change in Higher Education?: A case study relating models of organisational change to e-learning implementation. Journal of Higher Education Policy and Management, 27 (1), 81-96.

[26] Dietinger, T. (2003). Aspects of e-learning environments. Graz University of Technology.

[27] El-Khatib, K., Korba, L., Xu, Y., & Yee, G. (2003). Privacy and security in e-learning. International Journal of Distance Education Technologies, 1(4), 1-19.

[28] Friedman, B., Khan Jr, P. H., & Howe, D. C. (2000). Trust online. Communications of the ACM, 43(12), 34-40.

[29] Furnell, S., & Karweni, T. (2001). Security issues in online distance learning. Vine, 31(2), 28-35.

[30] Furnell, S. M., Onions, P., Knahl, M., Sanders, P. W., Bleimann, U., Gojny, U., & Röder, H. (1998). A security framework for online distance learning and training. Internet Research, 8(3), 236-242.

[31] Graf, F. (2002). Providing security for eLearning. Computers & Graphics, 26(2), 355-365.

[32] Gunasekaran, A., McNeil, R. D., & Shaul, D. (2002). E-learning: research and applications. Industrial and Commercial Training, 34(2), 44-53.

[33] Hagen, J.; Albrechtsen, E.; Johnsen, S. O. (2009). The long-term effects of information security e-learning on organizational learning. Information Management & Computer Security, 19 (3), 140 – 154.

[34] Hassanzadeh, A.; Kanaani, F.; & Elahi, S. (2012). A model for measuring e-learning systems success in universities. Expert Systems with Applications, 39 (12), 10959-10966

[35] Harauz, J. Kaufman, L. M., Potter, B (2009) Data security in the world of cloud computing. IEEE Security & Privacy, 61-64.

[36] Hoglund, G.; McGraw, G. (2004). Exploiting Software: How to Break Code. Boston, Mass.: Addison-Wesly.

[37] Holsapple, C. W.; & Lee-Post, A. (2006). Defining, Assessing, and Promoting E-Learning Success: An Information Systems Perspective. Decision Sciences Journal of Innovative Education, 4(1), 67-85.

[38] Karadsheh, L. (2012) Applying security policies and service level agreement to IaaS service

model to enhance security and transition. Computers & Security, 31 (3), 315-326.

[39] Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J. and Guilick, J. (2008). Security considerations in the system development life cycle, National Institute of Standards and Technology, Gaithersburg, MD.

[40] Kritzinger, E,; & von Solms, S. H. (2006). E-learning: Incorporating Information Security Governance. Issues in Informing Science and Information Technology, 3, 319-325.

[41] Kroenke, D. M. (2011). Using MIS, 3rd ed. Prentice Hall.

[42] Kumar, S., Gankotiya, A. K., & Dutta, K. (2011). A comparative study of moodle with other e-learning systems. Paper presented at the 3rd International Conference on.Electronics Computer Technology (ICECT).

[43] Lahoud, H. A., & Tang, X. (2006). Information security labs in IDS/IPS for distance education. Paper presented at the Proceedings of the 7th conference on Information technology education.

[44] Lawhon, T., Ennis-Cole, D., Lawhon, D. C. (2006). Copyright laws and fair use the digital era: Implications for distance education program in community Colleges. Community College Journal of Research and Practice, 30, 479–483.

[45] Lennon, M. (2011, July 13). Booz Allen Hamilton confirms cyber attack on learning, management system. Retrieved from http://www.securityweek.com/booz-allen-hamilton-confirms-cyber-attack-learning-management-system

[46] Li, M., Lou, W., Ren, K. (2010). Data security and privacy in Wireless Body Area Networks. IEEE Wireless Communications, 51-58Masud, M. A. H.; Huang, X. (2012). An e-learning system architecture based on cloud computing. Engineering and Technology, 62, 74-78.

[47] Limayem, M., & Cheung, C. M. (2011). Predicting the continued use of Internet-based learning technologies: the role of habit. Behaviour & Information Technology, 30(1), 91-99.

[48] Lin, N. H., Korba, L., Yee, G., Shih, T. K., & Lin, H. W. (2004). Security and privacy technologies for distance education applications. Paper presented at the 18th International Conference on Advanced Information Networking and Applications.

[49] Masud, M.A.H. and Huang, X., "An E-learning System Architecture based on Cloud Computing," World Academy of Science, Engineering and Technology, 62. 74-78. 2012.

[50] Mensche, S.; Wilkie, L (2011). Information Security activities of College Students: An Exploratory Study. Academy of Information and Management Sciences Journal, 14(2), 91-116.

[51] Mohammadi, H. (2014). Investigating users' perspectives on e-learning: An integration of TAM and IS success model. Computers in Human Behavior, 45, 359–374.

[52] Nickolova M. and Nickolov E. (2007). Threat model for user security in e-leaning systems. International Journal "Information Technologies and Knowledge", 1, 341-347.

[53] Ong, C.-S., Lai, J.-Y., & Wang, Y.-S. (2004). Factors affecting engineers' acceptance of asynchronous e-learning systems in high-tech companies. Information & Management, 41(6), 795-804.

[54] Ozkan, S. & Koseler, R. (2009). Multi-dimensional students' evaluation of e-learning systems in the higher education context: An empirical investigation. Computers & Education, 53, 1285-1296.

[55] Panko, R. (2010). Corporate computer and network security. Prentice Hall, Upper Saddle River, NJ.

[56] Raitman, R., Ngo, L., Augar, N., & Zhou, W. (2005). Security in the online e-learning environment. Paper presented at the Fifth IEEE International Conference on Advanced Learning Technologies, Kaohsiung, Taiwan.

[57] Reece, R. P. & Stahl, B.C. (2015). The professionalisation of information security: perspectives of UK practitioners. Computer Security, 48, 182-195.

[58] Rhee, H. S., Ryu, Y. U., & Kim, C. T. (2012). Unrealistic optimism on information security management. *Computers and Security*, *31*(2), 221-232.

[59] Rjaibi, N.; Rabai, B. A.; Aissa, A. B.; & Louadi, M. (2012). Cyber Security Measurement in Depth for E-learning Systems. International

Journal of Advanced Research in Computer Science and Software Engineering, 2 (11), 1-15.

[60] Rocha Flores, W., Antonsen, E., Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security, 43, 90-110.

[61] Rani, N., Suradi, Z., & Yusoff, N. (2014). An analysis of technology acceptance model, learning management system attributes, e-satisfaction, and e-retention. International Review of Management and Business Research, 3(4), 1984-1996.

[62] Saadé, R., & Bahli, B. (2005). The impact of cognitive absorption on perceived usefulness and perceived ease of use in on-line learning: an extension of the technology acceptance model. Information & Management, 42(2), 317-327.

[63] Salmon, G. (2005). Flying not flapping: a strategic framework for e-learning and pedagogical innovation in higher education institutions. Research in Learning Technology, 13(3), 201-218.

[64] Sánchez, R. A., & Hueros, A. D. (2010). Motivational factors that influence the acceptance of Moodle using TAM. Computers in Human Behavior, 26(6), 1632-1640.

[65] Sandhu, R.S., Coyne, E.J., Feinstein, H.L. and Youman, C.E. (1996). Role-based access control models. Computer, 29 (2). 38-47.

[66] Saxena, R. (2004). Security and online content management: balancing access and security. IEEE Conference,

[67] Selim, H. M. (2007). E-Learning critical success factors: Critical success factors for e-learning acceptance: Confirmatory Factor Models. Computers & Education, 49, 396–413.

[68] Shankar, V., Urban, G. L., & Sultan, F. (2002). Online trust: a stakeholder perspective, concepts, implications, and future directions. Journal of Strategic Information Systems, 11(3), 325-344.

[69] Shiau, W.-L., & Chau, P. Y. (2016). Understanding behavioral intention to use a cloud computing classroom: A multiple model comparison approach. Information & Management, 53(3), 355-365.

[70] Sood, S. K. (2012) A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35, 1831–1838.

[71] Sumak, B., Hericko, M., & Pusnik, M. (2011). A meta-analysis of e-learning technology acceptance: The role of user types and e-learning technology types. Computers in Human Behavior, 27(6), 2067-2077.

[72] Stella, A. and Gnanam, A. (2004). Quality assurance in distance education: The challenges to be addressed. Higher Education 47, 143–160.

[73] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 425-478.

[74] Weber, B.; Reichert, M.; Rinderle-Ma, S. (2008) Change patterns and change support features – Enhancing flexibility in process-aware informationsystems. Data & Knowledge Engineering, 66(3), 438–466.

[75] Weippl, E., Ebner, M., & Austria, S. B. (2008). Security & Privacy Challenges in E-Learning 2.0. Paper presented at the Proceedings of E-Learn.

[76] Yong, J. (2007). Digital Identity Design and Privacy Preservation for e-Learning. 11th International Conference on Computer Supported Cooperative Work in Design, Melbourne, 858-863.

[77] Zafar, H., Clark, J.G., Ko, M. and Au, Y.A. (2011). Critical Success Factors for an Effective Security Risk Management Program: An Exploratory Case Study at a Fortune 500 Firm. in Proceedings of the Seventeenth Americas Conference on Information Systems (AMCIS), Detroit, MI, 11.

[78] Zhang, D., Zhao, J. L., Zhou, L., & Nunamaker Jr, J. F. (2004). Can e-learning replace classroom learning? Communications of the ACM, 47(5), 75-79.

[79] Zhao, J. J., Alexander, M. W., Perreault, H. Waldman, L.; Truell, A. D. (2009). Faculty and Student Use of Technologies, User Productivity, and User Preference in Distance Education. Journal of Education for Business, 84(4), 206-212.

[80] Zuev, V. (2012). E-learning security models. Management, 7(2), 24-28.