CREATING A SAFER ONLINE LEARNING ENVIRONMENT FOR STUDENTS AND PROFESSORS: CYBERSECURITY IN ONLINE LEARNING ENVIRONMENTS

by

Saturlino Leandro

A project report submitted to the Faculty of Education

In conformity with the requirements for

The degree of Master of Education

Queen's University

Kingston, Ontario, Canada

September, 2013

Abstract

This project report is a design of an online security investigation from the perspective of professors and students, to provide information to higher educational institutions that would help them prepare professors and students to work securely online. Therefore the project has the secondary purpose of creating a safer online learning environment for students and professors.

Post-secondary educational institutions are responding increasingly to demands for online distance education, demands fuelled by the exponential growth of the Internet and associated information and communications technology (ICT) (Fan, 2011; Homeland Security Digital Library (HSDL), 2009; Kingkade, 2013; Rudestam & Shoenholtz-Read, 2010). As institutions increase their dependence on the Internet to deliver courses to students online, they encounter rapid growth in malicious online activity, which happens literally everyday (European Commission, 2013; Johnson, 2005; Orrey, 2010; Shaeffer, 2009). Literature on the security of online education has acknowledged this fact (Adams & Bradford, 2003), but offers little guidance for protection.

Every online education stakeholder has responsibility to ensure safety online. Administrators depend on ICT professionals to meet most of their security needs, but professors and students also have responsibility for security and may need guidance and support. The results of inadequate security can be catastrophic, leading to loss of trust and revenue (European Commission, 2013; Kovacs, Markam & Sweeting, 2004; Kennedy, 2011). E-Learning demands change in curriculum and in attitudes from the traditional educational system to the new online distance education (Zhang & Nunamaker, 2003).

Professors and students need to be protected online; they also need to feel free to choose computer programs and applications that facilitate online learning. Balance is required in addressing the needs of professors and students versus those of the administrators of institutions of higher education (Power, 2008).

This study addresses the following research questions: What online security problems do professors and students face? What do they know about online security? What steps do they take to protect themselves? What are the gaps between their security knowledge and practice? How do professors and students learn about online security problems, and what can they do to address these problems?

The design uses a qualitative research methodology. The proposed data gathering consists of interviews and a focus group (McMillan & Schumacher, 2010), all conducted online. The interviews and focus group discussions will be recorded and the collected data later analyzed using NVivo software. The outcome of this project report is a design of research to guide those working in higher-education institutions to support professors and students in the safe use of the internet.

Acknowledgements

I would like to register my gratitude to the many individuals who have made this project, including the completion of my graduate studies, possible. These people have helped me directly or indirectly in undertaking the graduate study program in Education. Without them, I might not have completed this study and the project. They gave me valuable, friendly, moral, emotional, and academic support and advice when I need it the most.

The first group include my supervisory team. I specifically would like to thank my supervisor Dr. William Egnatoff, whose support and supervisory work encompassed my graduate academic studies; he guided me through the project from the beginning to its completion. His valuable advice began in the summer of 2011, before I officially started my M.Ed. courses. I will ever be very grateful to him for his patience and for suggesting the appropriate course of action to be taken to make the research project conform to the standards of the American Psychological Association. The second member of the supervisory team I must thank is Dr. Richard Reeve, who has been instrumental in his advice during and throughout out the span of this project. He advised me on what specific curriculum elements to be included in the project. My thanks also go to all other instructors whose courses I attended: they challenged me and provided critical appraisal in my studies and suggested improvements that guided my academic writing, research skills and knowledge acquisition.

The second group of individuals I must thank include librarians from the Queen's University Education Library and also the administrators and administrative assistants at

the Office of Graduates Studies, Faculty of Education, Queen's University: Specifically I am grateful to Marlene Sayers who helped a lot with the M.Ed. program and the administrative assistants: Celina Caswell, Erin Wicklam, and Yonna Sayili. They constantly reminded me of important program information, updates and deadlines. The librarians Dr. Corinne Laverty and Brenda Reed and other librarians helped me with all the information I needed for my courses and project. Sometimes I received from them specific course lessons on the use of special library software to access and use online library information sources.

The third group include my family and friends, who have given me emotional support and parental advice in my academic journey. I thank my parents for instilling in me the ideas of hard work and of not flinching before difficult tasks. They believed in the benefits of education, especially higher education, and have encouraged me to go as far as possible in this academic journey. My friends at Queen's University and those outside the University contributed to the success of the program by giving me friendly advice on different course choices, or by working collaboratively with me on given course projects and assignments.

Lastly but not least, I thank those who have contributed to the success of this project and to the completion of my M.Ed. study program in one way or another. I will always be grateful to you for what you have done. Even if I have not personally met you, I say thank you for your support.

Table of Contents

Chapter 1

Introduction

The exponential expansion and development in computer and the worldwide web technology has lead to the widespread adoption of the internet as a medium of communication and information exchange. As a result, higher education institutions have adopted the internet to offer online courses so as to stake their claim on the potentially large, growing, and profitable market of online education (Anderson, 2008; Adkins, 2009; Bates, 2010; Eduventures, 2013; Green & Wagner, 2011; Kim & Bonk, 2006; Nagel, 2010). Nagel (2010) specifies the unprecedented market growth of electronic learning to be $27.1 billion, projecting it to double to $49.6 billion by 2014. Online distance education is also convenient and cost-effective (Bates, 2011; Belawati, 2006; Caswell, Henson, Jensen &Wiley, 2008; Meyer, 2008; Rickard, 2010). But as computers and other communication devices are used to leverage the great resource of the information and communication technology for learning and teaching purposes, the two groups of stakeholders encounter serious threats brought about by heavy reliance on these computers and the internet technology to deliver online courses (Academic Partnerships, 2011; Alwi, 2012; Billo & Chang, 2004; Cook, Conti & Raymond, 2012; Denning, 2007; Issues Monitor, 2011; Stacey, 2009; U.S. Department of Defense, 2011). Sometimes the threats lead to emotional and psychological injury or death (Johnson, 2005; Potaros, 2012; Royal Canadian Mounted Police, 2013; Willard, 2007).

One of the consequences of the rush to adopt the internet as a medium of online course delivery is the disregard of the importance of cybersecurity, which costs the United States alone US $100 billion per year (Gorman, 2013). Jackson, Jickling and Webel (2004) estimated the annual worldwide cost of all forms of cyber attacks to be $226 billion, quoting the 2003 figures reported by different computer security firms; and just viruses and worms alone cost a staggering amount of $13 billion. Kovacs et al. (2004) gave a lower estimate of $18 billion annual worldwide cost of major virus attacks; and in Canada alone, he put the annual financial losses at $1 billion to $2 billion Canadian. These figures demonstrate that there is a hefty price to be paid to do business online, which includes e-learning (Nagel, 2010). As internet users, the students and to some extend the professors, pay this price in two ways: financially, when they pay to study online, and emotionally and psychologically, when they suffer identity theft due to virus and other cyber attacks.

Purpose

The purpose of the proposed study is twofold: first, to create awareness of cybersecurity knowledge and practice with respect to the two stakeholder groups, students and professors, and second, to give institutions of higher learning information of relevance to the protection of the privacy of their students and professors against online threats, intrusion and attacks. It might also give these institutions information of relevance to increasing the safe use of online learning spaces that they do not maintain themselves.

Rationale

The proposed research looks at the role of two groups, students and professors, in ensuring data integrity and the online protection of their privacy and confidentiality. Students and professors are the focus of this study design because they constitute the largest groups that are involved in online learning, teaching, and training. In online coursework and training, students and professors expose themselves to various kinds of cyber-risks, threats, attacks, identity theft, and exploitation (Johnson, 2005).

Professors are at the forefront of the design, implementation, and delivery of online courses. They have to make difficult decisions concerning the choice of software, hardware, and educational computer programs and web applications that they consider secure and appropriate for the courses they have to teach online. However, they often meet with conflicting decisions taken by higher education administrators who prefer one set of online education computer applications and programs to the ones already chosen by these professors. The administrators often rely on the advice of information technology personnel, who are not trained in the art of pedagogy. Sometimes professors become frustrated because they cannot have the freedom of choosing the software programs and applications that they would like to use to facilitate online teaching and learning. In talking about the constant and sudden change brought about by the need to migrate to online learning, Davis (2004) specified the issue that exists between administrators of higher education institutions on the one hand, and the professors and the students on the other.

For students, the choices do not exist in that they must use the programs and course management (CMS) software and LMS suggested by their intuitions. Sometimes these students use social media software and networking sites to communicate and exchange ideas amongst themselves, their professors, librarians, supervisors, researchers, and other staff from their intuitions. They may either accept the restrictions placed on their choices of software, or go elsewhere to take their online courses. These social networking sites are often insecure.

Incidentally, during the planning of this research project design, the author suffered identity theft: he became a victim; he was part of a group of 583,000 Canadian student-loan recipients, whose privacy was breached by the loss of a hard drive from the Canadian Federal Government's Office in Gatineau, Quebec. In November 2012, the hard drive was stolen; it contained all the personal data of the students. It took the Federal Government 3 months to notify the students about this incident, during which time the thief or thieves might have produced all sorts of identities, impersonating the victims or creating other threats from the stolen data. Personally, I have suffered additional emotional distress related to the theft of my personal information. Other students may have suffered similar or worse distress as a result of this theft (Johnson, 2005).

A number of measures have since been taken following the breach of security at the Federal Government's Office in Gatineau, Quebec: the Minister responsible at the time ordered the training of her staff to seriously handle computer security issues; this is too late. A class action lawsuit has been started in Newfoundland and Labrador (Rennie, 2013), alleging negligence by the Federal Government or that the staff that kept the hard

drive may have been complicit in the theft. If the lawsuit is successful, it could cost the Federal Government millions of dollars in compensation to the student victims (Calgary Herald, 2013 & CBC News, 2013).This is just one incident of computer theft that has caused disaster to the students and to the Canadian Federal Government.

This proposed research does not address security as a whole; it concentrates on online security related to teaching and learning through online courses. The nature and extent of the data security problem as faced directly by students and professors is not known. The researcher was unable to find research documenting the extent of the problem as faced by students and professors, their practices in protecting themselves, and their knowledge upon which those practices are based.

The researcher has decided to undertake this research design on the role and perceptions of students and professors towards cybersecurity as they engage in the positive use of the internet for educational purposes. The researcher believes they ought to be able to do this without hindrance or threats of identity theft or cyber attacks. Unfortunately, online distance education, which is about to become indispensable to online academic communication and to the acquisition of knowledge and skills, is being convoluted by hackers, hacktivists, social vigilante groups, organized crime, and also some companies and state secret services organizations (European Commission, 2013; Fowler & Cronau, 2013; Hypponen, 2012; Rubin, 2012; Johnson, 2005). The researcher is passionate about the use of ICT in all its forms to facilitate learning, especially online learning.

Electronic learning has become a level playing field, enabling most students to learn at a distance, anytime and anywhere, provided that the resources like computers, smartphones, tablets, iPads, and internet infrastructure are available. The researcher feels that students and professors should be protected from cyber attacks. Training and other approaches to protection should be based on research that reveals how much students and professors know about online threats and risks and what to do to protect themselves. This study is designed to reveal: (a) how much students and professors know about cybersecurity; (b) the frequency, magnitude, persistence, and severity of attacks; (c) how widespread is the culture of denial of cybersecurity attack; and (d) what ideal training programs are urgently required to equip students and professors with the skills and knowledge they need to protect themselves and their resources in the online learning environment (CyberPatriot, 2013; European Commission, 2013; Fowler & Cronau, 2013; Manson, 2013; Polycentric, 2013).

Online distance education is growing very fast (Anderson, 2008), and not enough security information and training are being provided to those who want to use it as the new medium of knowledge and skills acquisition (Hwang et al., 2012; Rudestam & Schoenholtz-Read, 2002). The internet as a medium of communication is no longer an innocent place as it once was (Carter et al., 2002). It has become a goldmine for cyber criminals (Kennedy, 2011). The researcher feels the need to contribute to the protection of unwary students and professors through dissemination of research findings.

This study seeks to contribute knowledge to uphold personal privacy online for those who aspire to take courses and learn new skills using the internet. The researcher

also plans this study to be a small contribution to celebrate human ingenuity as society advances technologically. This study could have some impact on motivating stakeholders to take protective measures while studying or teaching online. No one should have the right to interfere with the learning process or the surfing habits of individuals in an online environment, be it for education, business, or provision of essential services.

The study of cybersecurity in relation to the field of online education is relatively new. The study is timely because online distance education is expanding at an exponential rate (Rudestam and Schoenholtz-Read, 2010). The next section presents and elaborates upon the research questions.

Research Questions

There are five research questions that guide the proposed study of security related to the experience of professors and students engaged in online learning and teaching. Since this group of stakeholders is divided into two, the questions will be formulated according to this categorization. In studying security in relation to professors, my concern is on matters related to online teaching. For students, my concern will be on matters related to learning and communications online and interaction amongst the students themselves, between the students and professors, and between the students and administrators of higher education institutions.

The research questions that guide the proposed research design are as follows.

1. What security problems have professors and students encountered while using the internet for educational purposes? This question concerns specific online security issues that professors and students encounter as they pursue online education. The study

anticipates serious disasters that might have occurred in the recent past, or that are taking place at present, either caused by malfunction or by outside interference. The study will look for past experiences that involved data lost by accidental deletion or by willful destruction of data by hackers, or through stolen laptops and other devices such as tablets, and desktops. It will consider data lost because of damaged operating systems and other vital computer applications. It will gather data on stakeholders' awareness of attacks on them by viruses, Trojan horses, phishing, pharming, blackmail, bullying by imposters, and so on. Activities of hacktivists or vigilante social hacker anonymous groups or other online criminals will also be taken into account in this study. In addition to these data, the study will look at stolen copyright material, and Denial-of-Service attacks, destruction of network systems leading to loss of business or training opportunities. Another interest in this study is the emotional damage that these stakeholders experience after a serious attack or destruction of personal data. In this study, in particular, the researcher will gather information on the circumstances that the participants were in when they encountered attacks and experienced loss of data; and what software, application, and computer systems they were using at the time of the attack or theft.

2. What do professors and students know about online security in relation to their use of the internet for teaching and learning? The researcher will examine and discover the computer operating systems and software that the participating students and professors use when they go online to study or teach. The researcher will also explore in this question the online security perceptions, attitudes, and awareness of these stakeholders and their ability to detect existing and emerging cyber threats.

Students studying online, under certain professors, must also keep the same confidentiality as do the professors. If they are reckless and do not know their role in keeping the online study environment safe, could they unwittingly contribute to the destruction or theft of their personal data and that of their professors? This research project will also try to find out what professors know about their role in preventing online security breaches to their confidential personal data and that of the students. The same issue applies to the students. One of the questions that must be dealt with here is whether the stakeholders, professors and students, know about the common attack methods and programs used by hackers. How much do they know about fake websites used by criminals to lure unsuspecting internet users to their destructions? What do they know about dangerous email attachments from unknown senders? What do they know about the types and sources of threats to data integrity and access? What do they know about the methods required to protect themselves from these threats? Are they bothered by unauthorized destruction of their computer property, or the theft of their confidential personal data? Are they confident about the cybersecurity protection measures provided by their institutions? Have their institution informed them of any security breaches? The research will try to pinpoint what students and professors consider good online security practice and whether they strictly follow the methods they consider safe online practice. What do they consider unsafe cybersecurity practice? Can they distinguish direct attack from the malfunction of their computer systems?

3. What steps do professors and students take to protect themselves against online security threats? In other words, what extra security measures do they take to protect their

computer systems and computer applications from unwanted and unauthorized intrusion by hackers and other criminal elements? This question will address the specific steps that students and professors take to defend themselves and the resources that they employ or use to access online learning and teaching respectively. It will help the research to discover the resourcefulness of the stakeholders in finding ways to eliminate the online threats by seeking additional resources and any available protection methods that they know can help them. Some of the steps that the researcher anticipates are as follows: the unsafe disposal of unwanted old hard drives to wipe off all traces of stored data; being proactive to understand and educate oneself about the methods used by online attackers to infiltrate any computer system and cause havoc to it, and to any data that might have been stored on it; updating antivirus and other necessary software to stay ahead of malware and viruses or Trojan horses; monitoring one's computer system performance to detect unauthorized activities on their system; changing passwords and usernames frequently and protecting other software using programs such as emails with encryption methods; taking measures to back up one's data from to time to avoid accidental permanent deletion or the destruction of data, computer system and other applications; reporting all suspicious activities to their institution's IT department, to the University or College administrators, or to the computer forensic law enforcement officers; always logging off any computer system and application after use to avoid leaving them open or vulnerable to attacks; and reading and learning about the latest information concerning new malware and online attack threats and methods, and how to defend against them, such as by getting up to date information from security and other media and

organizations, including Common Weakness Enumeration (CWE) (2011), National Vulnerability Database (2011) and The Open Web Security Application Project (OWSAP) (2013).

4. What is the nature of the gap that exists between the knowledge of good online security practice that the two stakeholders know and the actual practice that they exercise? This question will explore the discrepancy that exists between actual practice and the knowledge of good online security practice that is necessary to thwart problems before they happen. Knowing the gaps will guide institutions in working to improve both relevant knowledge of security and safe practice. This will allow the researcher to examine the choices relative to the risks and the knowledge on which these choices are based. Addressing this question can inform the researcher of the fact that past experiences of users can have either negative or positive consequences on their views towards cybersecurity. That is if they experienced disasters in the past, they might have changed their behavior when considering this issue. It can also inform the researcher of what the users or stakeholders consider worth protecting.

5. How do professors and students learn about online security problems, and what can they do to address them? What is the role of the higher education institutions in providing security information to students and professors for the learning management systems (LMS) that they control to aid professors and students? The researcher will elicit from participants, students and professors, information concerning the way they discover online security problems either through personal experience, or through the experiences of others that they perceive as relevant to their situation. For example, if one of their

colleagues has been attacked, they may take that information into account and then take steps to protect themselves. Besides, they can study relevant data to know the strategies and methods used by hackers and other online criminals to execute the attacks. As a researcher, I am interested to know these steps and how participants adopt and apply them to particular situations. The researcher will attempt to find out whether students and professors have attended any computer security workshops or courses as part of their vigilance against cybersecurity threats and attacks. The researcher will also investigate the communication methods that students and professors use amongst themselves, and whether these communication methods use encryption.

Project Report Overview

This project report is organized into three chapters. The first chapter introduces the study and its purpose and significance, provides a background on online distant education and cybersecurity, and helps to explain my interest in studying this topic. The second chapter contains a review of the existing literature on online learning and its relation to cybersecurity. It situates the proposed study in relation to the existing literature. The third chapter contains the methodology used to answer the research questions. The data include recordings and notes of interviews and a focus group with students, and of interviews with professors. The chapter gives details of participant selection, the methods for data collection and analysis, and a discussion of trustworthiness and limitations.

Chapter 2

Literature Review

The project report draws upon literature concerning creating a safer online learning environment for students and professors. This chapter deals with the literature on online distant education and cybersecurity. The review examines the literature on this topic and the gaps that exist with respect to the research questions. The chapter concludes with the implications of this review of the literature that led the researcher to study this topic of e-learning and cybersecurity.

The chapter also describes the main conflict that arises between professors and administrators of the institutions of higher education: The professors would like to choose, without restrictions, any secure software and web applications that they know supports online learning; they would also like to use free Open Source software, or to experiment with the latest CMS and LMS applications, but administrators often prefer different software and operating systems, depending on the cost of licensing or in order to maintain their affiliation with certain computer or software corporations and other companies (Anderson, 2008).

According to Davis (2004), the constant flux in staff work, brought about by online learning, means that many of these staff members receive little or no official training: at times, they successfully learn on their own. He further warned the administrators against exploiting these knowledgeable staff, and argued that institutions must provide additional training to them because of the opportunities that online learning

has provided (pp. 44). He also added that, in deciding resource allocation for online learning, authorities need to carefully strike a balance between three groups: the decentralized expert technical staff, who want the freedom to choose one approach over another; the centralized administration who know little or nothing, but are equally responsible for the success and efficacy of the system, and the users who consist of students and teachers (Davis, 2004, pp. 45).

The literature review in this project report is designed according to each research question. There are five research questions that follow. The review will begin with the first one.

Question One: Online Security Problems. What cybersecurity problems have students and professors encountered while using the internet for educational purposes?

The problems faced by students and professors regarding online security are the same as those faced by other general internet users. Stallings and Brown (2012) claim that internet users often take online security for granted, until a serious attack incident happens; and in their design, they argue, network administrators often treat cybersecurity as an afterthought, viewing it as an obstacle to efficiency (Stallings & Brown, 2012).

Stange (2011) believes that "concerns about privacy may have an effect on student learning" (p. 2). Hackers can disrupt the online interaction between students, their professors and administrators of higher education institutions. For example, they can cause Denial-of-Service (DoD) attack, which causes students and professors to worry (Abawajy & Kim, 2010; Stange, 2011), further affecting their online performance

(Wagner, Hassanein & Head, 2008). The researcher is interested in these groups of stakeholders and how they encounter and handle attacks; other students who study on their own are excluded from this study (Tallent-Runnels et al., 2006).

Some of the major threats to confidentiality, data integrity, and availability of applications and computer systems are the following: theft of personal information; spyware, malware, viruses, Trojan horses, harassment, online bullying, corruption of data, system or application crashes and failure, unauthorized access to copyright materials, and intrusion (Hwang, Fox, Jack & Dongara, 2011; Jackson et al., 2004; Johnson, 2005; Stallings & Brown, 2012). Carter, Faircloth and Lobe (2002) claimed that it is no longer possible to conduct any activity online without encountering threats and other risks. Kennedy (2011) emphasizes that the internet has become a goldmine for cyber criminals. Some researchers claim higher education institutions have abysmal records when it comes to the issue of providing online security protection to their students and staff (Dykman & Davis, 2008; North, George & North, 2006). Rubin (2012) specifies that any device can be hacked, no matter who manufactures it, or where it is manufactured. Starlings and Browns (2012) assert that any web application (websites) can be compromised easily. Shaeffer (2009) stressed that cyber attacks happen literally every day; and these attacks target businesses dealing with the swiping of cards. Cleef, Pieters, and Wieringa (2009) expressed fear that data centers (virtualization data storage centers) are not secure. Cyber criminals could gain access to such centers and preempt and steal research data or sabotage the attempt to discover certain elusive ideas like the Higgs boson (Chen, Nojiri and Streethawong, 2010).

The inability to backup data or not backing up computer systems and applications is another concept that is included in the group of problems that users, students and professors in this case, encounter very often. If there is no backup when disaster strikes, personal data, computer operating systems and other applications may be lost forever; only data recovery mechanisms can help to retrieve the data lost, and it often involves hefty cost. In some cases, the lost data may not be recovered at all.

Question Two: Knowledge as a Source of Defense. What do students and professors know about cybersecurity?

There is a real exponential growth in Information and Communication Technology (ICT), which has been fueled by the rapid growth in internet technology. As a result, educational institutions have tried to tap into its perceived benefits (Hwang et al., 2012; Rudestam & Schoenholtz-Read, 2010; Velte, Velte & Eisenpeter, 2010). Increased use of the internet by students and professors increases their risks and vulnerability to attacks, which is why there is a need to know about these risks and how to avoid or defend against them.

Students and professors vary widely in what they know about cybersecurity. The Students and professors, who are working in fields such as computer technology, computer security, and computer programming, know a lot about online security because of the nature of their work and study. They know the vulnerable areas of computer systems and weak software applications and leaking programming codes that may cause exploits (Carter et al., 2002; CIS, 2011; CWE, 2011; National Vulnerability Database, 2011; OWASP, 2012); they can tell if hackers have attacked their system or if an intruder

has interfered with their applications and programs. Other students and professors know very little or nothing at all about computer security, computer programming, or software development. They are most vulnerable to online attacks and threats because they have no idea of the dangers and risks that exist online. Hackers can easily steal their identities or damaged their computer systems and other software applications. They may know about firewalls, and may be familiar with the cursory messages given to them by their higher education institutions about computer security, but they cannot tell that they have been attacked or that they are being tracked (Hypponen, 2012; Kovacs, 2012; Orrey, 2010; Rubin, 2012).

The idea of rapid and widespread internet expansion in some parts of the world has exposed users to serious online threats (Alwi, 2012; Johnson, 2005; CWE, 2011; National Vulnerability Database, 2011). Students and professors who use the internet regularly for educational purposes face many potential online risks and threats because of their online activity. According to Canada's Cyber Security Strategy (2012), "Cyber security affects us all, in part because even attackers with only basic skills have the potential to cause real harm. Sophisticated attackers can disrupt the electronic controls of our power grids, water treatment plants and telecommunications networks" (p.1). A similar fear existed in the United Kingdom until, according to Campbell (2010), a strategy was developed to tackle cybercrime and cyber criminals. Therefore, concern about the devastating effects of cybersecurity by governments indicates that the dangers are real and cannot just be ignored or dismissed as hype.

This project report examines the ways students and professors protect themselves, which is the subject of next question.

Question Three: The Protection Mechanism. What steps do students and professors take to protect themselves against online attacks?

Before learning about the steps professors and students take to protect themselves in an online learning environment, it is important to define the enemy or enemies they are fighting against. European Commission (2013) cybersecurity proposal and strategy acknowledges the rapid growth in cybercrime, and the sophistication of cybercriminals and their networks. It states that "more than one million people worldwide" are affected or become victims each day (p. 9). According to Hypponen (2012) internet users, which includes students and professors, can be attacked online by three groups of people: organized criminals, vigilante groups or hacktivists, and state intelligence agencies or state governments. Some of these groups use advanced computer programs and methods to track, attack, hack, and steal or destroy data and computer systems (Rubin, 2012; Kovacs, 2012). Individuals and companies can also engage in secret attacks against internet users, which may include their adversaries. The motive of the attack can be monetary or economic gain, obtaining military or political power, or entertainment (Orrey, 2010). The nature of the attack can be very severe or mild, depending on the target and the individual or group that executes the attack.

There are some basic practices that professors must abide by or follow when dealing with students' confidential data both online and offline. According to the Office of Information Technology (OIT) (2012), under the Family Education Rights Acts

(FERPA), for example, professors must exercise due diligence to protect students' sensitive information and the awareness that relates their perspectives to cybersecurity. Jackson et al. (2004) and Johnson (2005) described confidential data that can be gathered from internet users, including students and professors. The sensitive data consisted of academic records, feedback, copyright material, and stored personal information: health information, insurance data, addresses, Social Security (USA) and Social Insurance (Canada) Numbers, telephone and cell phone numbers, curriculum vitae or resumes, etc.

How do students and professors defend themselves against advanced and knowledgeable enemies who threaten Internet security? This study will gather information about the level of knowledge students and professors possess and the specific steps they take to protect themselves and their computer systems and software applications. Those who study or are trained to teach computer security programs have an advantage over those who do not have any idea about how attacks are executed, or how malicious computer programs can be planted into their systems, without their knowledge.

The students and professors who have no knowledge of computer security usually depend only on a firewall, a default computer defense program that is included with the operating system. This is problematic because firewalls can be surpassed (Hypponen, 2012; Kovacs, 2012; Rubin, 2012; Sullivan & Liu, 2012). They may also depend on their institution's computer security network for protection (Johnson, 2005). Students and professors need to take extra online computer security measures besides those offered by their institution's computer security department, because former computer security employees and contractors, whose contracts have been terminated, could wreak havoc on

the privacy of these students and professors, or on the whole network of the institution (Abawajy & Kim, 2010; El-Khatib, Korba, Xu &Yee, 2003; North et al., 2006; Orrey, 2010). Sometimes higher-education institutions either give professors cursory security courses to prepare them to teach online, or give them no computer security training at all, yet ask them to delivery courses online (Willems & Meinel, 2012). The group that study and teach computer security rely on different techniques and methods to protect themselves: they have relevant knowledge as their first line of defense (CWE, 2011; OWASP, 2012); they run simulated attacks and then devise ways to defend against these attacks; they anticipate attacks and use several backups per month to prevent total loss of data; they do not download risky and dangerous programs or applications from unknown internet sources; they monitor the behavior of their operating systems and computer applications as these can indicate the presence of malicious software or possible unauthorized entry into the computer systems or applications; they frequently change their passwords and practice authentication methods: passwords, usernames, token biometric, and remote user authentication (Carstens, McCauley-Bell, Malone & DeMara, 2004; Stuttard & Pinto, 2011). They can manually remove viruses and Trojan horses that have infected their computer systems and applications. These are just a few of the many proactive procedures, methods, and techniques used by security-conscious online students and professors to protect themselves against the daily onslaught of cyber attacks.

The study will examine what contributes to the online security vulnerability of students and professors. The researcher will pay attention to the complex relationship between the research participants and their administrators, including decision makers in

information technology departments and their choices of computer applications and software to be used for online learning. Power (2008) disapproves of the restrictions placed by administrators on the learning management systems and other computer applications and platforms that professors and students prefer to use in an online study and teaching. These administrators worry about cost, licensing, and corporate-institutional affiliation; professors and students would like to have a free choice of Open Source platforms, operating systems, and the learning management systems that support e-learning. Power further explains the concerns that exist in distance education that "faculty, by and large, simply do not have the time or the incentives to devote themselves to learning new skills, mastering new technology and interacting with students in new ways" (p. 1). If faculty of higher education institutions are not interested in learning new skills in this respect, they will be very cautious and slow to adopt robust online security measures to protect those interested in online learning. Consequently, they will pay very little attention to online security; this will have a negative impact on the students and professors.

Some university and college administrators frustrate professors and students by placing restrictions on their choice of computer software, applications, and platforms because of monetary and proprietary concerns, thereby disregarding the importance of online security (North et al., 2006; Power, 2008; Orrey, 2010).

The literature in this section has revealed that students and professors who are experts in computer security learn about online risks, threats and attacks through active study, research and teaching practice; they take proactive security measures to protect

themselves when using the internet, both for educational and other purposes; they backup their data, computer systems and software applications to prevent catastrophic loss of data due to the activities of malicious hackers or computer system's failures or crashes. They can identify malicious programs from computer malfunctions.

Another group of students and professors who have no idea about online security do not know the risks and threats that exists in an online learning environment (Adams & Bradford, 2003). This group suffers serious consequences of not knowing the threats when they lose data and have their systems destroyed; sometimes their identities are stolen and they will not even identify the problem (CWE, 2011; Evans & Reeder, 2010; Johnson, 2005). Since they do not know the danger and the nature of the attacks, they cannot be concerned or take any protective measures.

Question Four: The Gap between Knowledge and Practice. What is the nature of the gap that exists between the knowledge of good online security practice that students and professors have, and the actual practice that they exercise?

The researcher has not been able to find any specific and reliable statistical literature regarding the nature and the magnitude of the gap that exists between knowledge and actual safety practices. Very little literature exists about what students and professors know and what they practice as far as safety online is concerned. Many higher education institutions have some computer security policies to protect their student population and employees, including the teaching staff. For example, Queen's University Computer User Code of Ethics places the responsibility on users to protect themselves: "Users are ultimately responsible for any and all use of their computing and network

accounts*"* (Queen's University Secretariat, 2005, p.1). The Athabasca University (2003) Policy and Procedures Manual states: "All staff or students who are not authorized to access its electronic networks and systems, or who exceed their authorizations, are also subject to the regulations outlined in this Policy" (p. 1). Some of the regulations in other higher education institutions may recommend logging off one's sessions, attending to one's laptops, tablets, smartphones in a library or public setting, etc. Although these general policies are geared towards respect for and proper use of the institution's computer and internet resources, the security sections are not backed up by training students and professors about security attacks (North et al., 2006). Moreover, many students may not even read or practice these policies; the research will examine the familiarity of participants with their institutions' policies. However, the knowledge and practice are different for students and professors who are registered and teach computer security from those who have no idea about cybersecurity. The study will examine the connections between what students and professors know and what they practice. This matter has not been addressed in the literature examined.

Question Five: The Methods of Learning about Cybersecurity. How do professors and students learn about online security issues and what do they do to address them?

The division of students and professors into those who have clear knowledge of online security and those who know very little or nothing at all continues through this section. Those who know very little or nothing about cybersecurity, learn about it the hard way. They often scramble to research about online security after a major disaster

attack that results in the loss of data, theft of intellectual property, corruption of the computer system or computer application or after financial loss due to online attack (Dorothy, 2008; El-Khatib et al., 2003; Orrey, 2010; Stallings & Brown, 2012). Since some of these students and professors do not know about cyber attacks, they do not worry about researching online security and its effects on their e-learning, or on their online teaching if they are professors (Alwi, 2012; Orrey, 2010). The problem is even compounded by the fact that cybersecurity is taken for granted by educators, while the cybersecurity criminals have become sophisticated in their methods of exploitation of the vulnerable (European Commissions, 2013; Fowler & Cronau, 2013). This point is emphasized by Grobler, Dlamini, Ngobeni and Labuschagne (2011), who describe the internet and the cyber world as "a dangerous place where innocent users can inadvertently fall prey to shrewd cybercriminals" (p. 7). Grobler et al. (2011) then asserts that a combination of factors, online dangers and irregular access to the internet technology, has exposed unsuspecting rural South African communities to cyber threats. The threats mentioned in this statement can be applied to the wider audience of internet users, which includes students and professors.

The other groups are those trained or undergoing training in computer security. These groups know the importance of online security. They know about issues caused by viruses, pharming, phishing, identity theft, online deception, etc. To address lapses in security, they follow strict procedures, methods and techniques to protect themselves online (Stallings & Brown, 2012).

Sometimes institutions do not teach about cybersecurity until they are ready to do so. Even so the cybersecurity courses are only taught to a small number of students who are interested in these types of courses. One such institution is the University of Maryland, which has started an "Advanced Cybersecurity Experience for Students (ACES), an undergraduate program, which they tout to be a "new model for cybersecurity education," the first in the United States (University of Maryland, 2013, p. 1). Specific programs like these are not meant to be taught to all students and professors, which is why most of them will not bother to take the time and initiative to learn about online security and its implications.

Cimons (2012) stresses the existence of CyberWatch, a Cybersecurity Training program for students at all school levels in the United States. These sorts of programs appear to be a product of an afterthought, hastily instituted after sustained, repeated, and damaging attacks to businesses and to people's privacy. She notes that:

> In recent years, enhancing cybersecurity has become a critical important issue with a growing sense of urgency. There has been an escalation in computer security attacks within the last decade, from so-called 'phising' scams that lure people into revealing sensitive and private information, to Internet attacks that crash popular websites. (p. 1).

She explains that the goal of CyberWatch is to train students for the cybersecurity industry (Cimons, 2012). This is how some students and professors learn about the importance of cybersecurity. The students do so by taking computer security courses,

while the professors acquire such knowledge through their own scholarly work and by teaching these courses to students.

To protect internet users in general, Schjølberg and Ghernaouti-Hélie (2009) advocated the formation of an international body to enact some laws to combat cybercrime and cybercriminals in cyberspace; they cited the convention initiative undertaken by international organizations such as the Council of Europe on Cybercrime, the United Nations Office on drugs and crime (UNODC), and the International Telecommunication Union (ITU) in the 1990s; it has since become outdated. They argued that:

> New methods of conduct in cyberspace with criminal intent must be covered by criminal law, such as phishing, botnets, identity theft, crime in virtual worlds, terrorist use of Internet, and massive and coordinated cyber attacks against information infrastructures. Many countries have adopted or preparing for new laws covering some of those conducts. (p. ii).

This indicates a concern from experts about the reality of online crime and its international nature, but it does not address the need for knowledge by stakeholders within educational institutions to protect themselves from existing cybersecurity threats. Those who are concerned about or teach and study computer security and computer programming, take into account this reality, and prepare for its impact. Those who do not care or who do not know the dangers of cybersecurity never prepare to protect themselves; and, as indicated by the preceding evidence, this is simply because they are ignorant of what lurks on the internet.

There are few programs undertaken by some institutions to create awareness amongst students and professors concerning the existence of cybersecurity threats and risks, and what to do about them. Fowler and Cronau (2013) report on the existence of foreign criminal syndicates that target Australian government and business entities. Although higher education institutions in Australia are not explicitly mentioned in this report, these hackers can easily target them if their computer networks are not properly protected.

In an attempt to spark cyber security motivation in students, Manson (2013) mentors and encourages students, even from secondary schools, to get involved in the Western Regional Collegiate Cyber Defense Competition. Other programs like CyberPatriot (2013) and Polycentric (2013) exist to spur students to learn more about online security, implying that, with the passage of time, they may become cybersecurity experts. This is one way students learn about this critical subject, but it affects only a small minority.

In summary, the students and professors learn about online security issues and what measures they ought to take to address them, depending on how much they know about cybersecurity. Expert professors trained in computer security learn about these issues through advanced computer security courses that they teach; the students who are enrolled in computer security courses learn about online attacks through active research. All other students and professors, who know very little or nothing at all, may learn about online security issues after a major attack incident. They may not even take any steps to

protect themselves or to remove the threats that may exist in their systems; which is why this research report is necessary to establish and corroborate these facts.

Implications for This Research Design

The emergence of e-learning as a serious alternative to traditional face-to-face form of education has caught education institutions off guard (Dabaj, 2011). Initially, universities, colleges, and K-12 schools viewed this form of distributed learning with reservation. With the exponential growth and expansion in information and communication technology, these institutions have now begun to embrace e-learning as a matter of necessity (Lewandowski, 2005; Kim & Bonk, 2006; Easton, 2007; Anderson, 2008; New Media Consortium, 2007; Rudestam & Shoenholtz-Read, 2010). The rapid development in ICT is itself fueled by the worldwide growth and adoption of the internet as a preferred medium of online communication (Fan, 2011; Ali & Elfessi, 2011). As post-secondary institutions come to rely heavily on the internet for virtually all their day-to-day computer operations and online course delivery, they overlook or disparage one important aspect of this communication: cybersecurity (El-Khatib et al., 2003; National Institute for Cybersecurity Education, 2011). Cyber attacks on computer systems, on computer applications, and on internet users have become a daily occurrence and have grown as rapidly as the internet itself (Alwi, 2012; European Commission, 2013). Malicious online activity includes but is not limited to, intellectual property infringement and copyright material theft, hacking for identity theft or to steal sensitive (personal, institution, company, and government) data, viruses, Trojan horses, phishing, pharming, financial fraud, and blackmail (Hathaway & Crootof, 2012; Johnson, 2005; Kennedy,

2011). Students and professors, who comprise a large group of online internet users for educational purposes, need robust online protection. This research design is part of a wider body of research that tries to raise security awareness amongst students and their professors and other internet users (Nance, Hay, Dodge, Seazzu & Burd, 2009).

This research project aims to investigate the perspectives of the students and professors with respect to cybersecurity to provide information to higher education institutions so that they may take serious and strong computer security measures to protect the students and professors. The report focuses on the online experiences of these two groups as they engage in their daily online studies and teaching, which must be done through the institutions of higher education. The online security issues are barriers that prevent professors and students from enjoying the full benefits of e-electronic learning (Berge, 1998). According to Breivik and Gee (2006), the internet has created a huge amount of information and made it available to students and professors. Having access to those resources free of security issues underlies the proposed research.

Chapter 3

Research Design and Methodology

This chapter describes the methodology to study the perspectives of students and professors about their understanding of, and actions related to, cybersecurity in higher education. The chapter describes and justifies the exploratory study technique, participant selection and recruitment, data collection and analysis, considerations used to ensure the trustworthiness of the study, and limitations (Attride-Stirling, 2001; Creswell, 2009).

The qualitative research approach appropriate for this study design is exploratory case study (McMillan & Schumacher, 2010). Qualitative study methods have been effective and successful in other research studies with a similar research problem (North et al., 2006). The justification for using this method comes from the need to undertake a study that addresses perspectives of professors and students about cybersecurity issues. The overall aim of the researcher is to contribute information that may lead to the promotion of online security for students and professors.

The study aims to develop a research outcome with clear guidelines for future research. Any researcher interested in this subject could use the findings of the proposed research to design studies to collect data from larger populations of professors and students to get more comprehensive answers to the questions of the proposed research in a wider variety of contexts.

In this research design, the researcher has decided to use both interview and focus group procedures. McMillan and Schumacher (2010) and Stake (2010) recommend the

use of in-depth interviews to gauge the perceptions, opinions, beliefs, and attitudes of participants. The focus group allows participants to express their views and share their experiences through discussion with other participants. The act of speaking freely triggers in other participants spontaneous accounts of experiences that would not have been remembered if they had not participated in such a group.

A small pilot study will be conducted to test and refine data gathering.

Participant Selection

The study involves higher education students and professors, two groups of stakeholders who are the main practitioners in e-learning. Since they teach or study online, they are expected to be familiar with working and communicating online. Recruitment and all data gathering will be done through online communication separate from any communication related to participants' online coursework.

The criterion for student participation is that they must have taken at least one course online from a higher education institution for a period of at least one semester. These students must be from higher education institutions and must study online; that is, they must either take all or some of their courses online. The students' status of being full-time or part-time does not affect their participation in this study. The criterion for professor participation is that they must have taught at least one course online at a higher education institution for a period of at least one semester. The professors' status of being full-time or part-time does not affect their participation in this study.

All participants will be chosen according to their willingness and availability to participate. Each of the participants should have a computer, uninterrupted internet access, and should be in a place free from distractions during data gathering.

Participants will all be chosen according to the qualitative research method of purposeful sampling. Participants will be chosen from three higher education institutions: two universities and one community college. One university will offer all or almost all of its courses online. The other will offer most of its courses face-to-face, but will also offer some courses entirely online. Courses taken by the student participants and taught by the professor participants must be at least one full semester long. Nine students will be chosen, three from each of the institutions. Three professors will be chosen, one from each of the three institutions. This sampling will allow comparison across three different institutional settings.

For the pilot study one professor from one of the three institutions and two students, one from the community college and the other from one of the universities, will be chosen. The pilot participants will not participate in the main study. The non-random, purposeful method of pilot group selection is "homogenous sampling," which is appropriate for this type of research design (Onwuegbuzie & Leech, 2007, p. 111).

The small size of the participant groups is a result of the nature of the research design: an exploratory study which seeks to gather data to answer specific research questions (Onwuegbuzie & Leech, 2007) as outlined in Chapter 1.

Data Gathering Procedure

Although participants' online teaching and learning experience may have been enriched by the use of multiple media (Balaji and Chakrabarti, 2010), a single medium, such as Adobe Connect or *Elluminate Live!* will be selected for online data gathering for all interviews and the student focus group session. The same medium will be used for the pilot study and the main study. Participants will be given necessary Web links and login instructions to use the medium.

The main data gathering will be preceded by a pilot study. The pilot study will be used for three purposes: to test the interview protocols for students and professors, to test the focus group protocol for students, and to test the use of the online medium used for gathering the interviews and focus group. This piloting process should give the researcher early indications of the success of the program in terms of how easy it is for participants to understand the procedures and how much time it takes, from start to finish, including the preparation. To test how to facilitate the process of the student focus group discussion, the researcher will refine the pilot focus group discussion design according to the data obtained from the analysis of the pilot interviews.

The sequence for the pilot study will be as follows: student interviews of approximately 20 minutes each; several days to summarize and analyze the interviews and prepare for the focus group; student focus group of approximately 30 minutes; professor interview of approximately 20 minutes; and finally, refinement of all procedures in preparation for the main study.

The sequence for the main study will be as follows: student interviews of approximately 60 minutes each; approximately one week to summarize and analyze the interviews and prepare for the focus group; student focus group of approximately 90 minutes; professor interviews of approximately 60 minutes each.

All participants would be identified using a code established by the researcher.

Recruitment

The researcher will contact Continuing Education or Distance Education offices at participating institutions in order to get the required number of student and professor participants. The researcher will try to have one contact person in each institution to facilitate the process of recruiting prospective participants. These helpers will be the ones to send out messages to invite participation and obtain contact information. All subsequent communication would be between the researcher and participants.

The participants would not have any close relation to the researcher. A letter of Information and Consent will be sent through email to the participants to read and sign. The participants can also give their consent orally online immediately prior to data gathering. The letter and consent form (Appendix D) will assure them of confidentiality, to the extent possible, in the handling of their personal data and will state their freedom to withdraw from participation in the research at any time.

The Data Gathering Instruments

All interview questions and details for focus group discussion are based on the research questions elaborated in Chapter 1. Protocols for the interviews and focus group are given in Appendices A, B, and C. There will be a total of 10 questions to be answered

within 60 minutes by the student participants in an interview; 5 questions to be discussed by the students in the 90-minute focus group; and 12 questions to be answered by professors within 60 minutes in an online interview.

The interview and the focus group processes will be recorded to facilitate data transcription afterwards; the participants will have the options of opting out if they feel uncomfortable before or during the course of the interview and focus group discussion. The participants are to be assured that no information concerning their identity will be divulged at any time during and after the research process. This will be cleared through the office of the Ethics Research Board. Knowledge and involvement in online distance education, coupled with the possibility of the experience of a cybersecurity attack are the determining factors in this interview (McMillan and Schumacher, 2010).

Pilot Interviews with Students

The two pilot students will be asked specific questions in their individual interviews. Each student will have three to five minutes to answer each of the three questions, including the prompts. At the end of the interview, each of them will have a minute to ask a question about online security or online study. The researcher will try his best to answer these questions. The researcher will control the process. The first question is about why they decided to take particular courses online. The second requires them to describe any online attack they suffered: What were they doing at the time of the attack? How severe was it? What steps did they take to resolve the problem? The third question is about any serious concern they have about privacy in any online learning environment. Why do they worry about it? What would be the likely solution for this issue? Finally,

the student will ask any question that troubles them about studying through the internet. The pilot interview should take about 20 minutes.

Pilot Focus Group with Students

The student pilot focus group will take approximately 30 minutes and will be conducted between three days and one week after the interviews are concluded and preliminary analysis is completed. The time and method of asking questions will be flexible. The researcher will adapt the facilitation of the focus group discussion according to the experience gained from the pilot interviews. The discussion will be done online, and will be recorded. The researcher will facilitate the discussion. Each participant will have a chance to contribute his or her views to the discussion. A similar approach will be taken with the main data gathering, but using the full protocol (Appendix B).

Pilot Interview with a Professor

The professor in the pilot study will be asked to describe (a) any expert computer security training that he or she has received before accepting online teaching assignment; (b) the magnitude, severity and frequency of any privacy or cybersecurity issue (s) that he or she has encountered while teaching online. What was the cost of the security breach in terms of money, time and effort? What has the experience of the attack incident taught him or her about taking pre-emptive, preventative and protective measures? (c) Any secure operating system that he or she prefers, and what security features differentiate it from the others.

Interviews with Students

The individuals with students will be conducted as in the pilot interviews, but with the full protocol (Appendix A), revised according to what was learned in the pilot study.

Focus Group with Students

The focus group will allow student participants to share their experiences in a live interaction, giving the observer the opportunity to see how students feel after a cyber attack, or to glimpse from the expression or tone in their voices, what practical knowledge and activities propel them to venture into areas that gets them into trouble: areas such as being redirected to visit compromised sites; downloading viruses onto one's computer system; answering hoax emails; and responding to secret financial appeals in social media. Can they detect fake websites from the real ones? Some of them may not know anything about cybersecurity, in which case the researcher will be able to listen to their voices, inflections, tone, hesitation and bewilderment, indicating that they are from the group that have no clue about identity theft, online attacks and why their computer applications crashes without warning. In this way, some of the answers to the research questions in this design will be elicited directly from what they say or even from what they fail to specify.

The order of discussion is the same as in the pilot study, but there will be additional probes so that participants may clarify and expand their contributions.

In the student focus group, participants will discuss questions that concern: (a) data integrity and confidentiality and how they feel about corrupted or compromised data;

(b) and what comes to their minds when they talk about online security. Probe: what does it mean to them? (c) What steps do they take to keep their online personal information secure? Probe: Have they suffered any security breaches? How did they feel about it? (d) Describe what they consider safe online practice? Probe: What exactly do they do to avoid being hacked? (e) What online security training have they received from their institution before they started their online studies? How robust was the training? Has that training been helpful to them? More probes will be asked if time allows.

Interviews with Professors

The interviews with professors will follow the protocol given in Appendix C. The researcher will specifically watch for conflict between computer software and applications that the professors prefer to facilitate online learning and those online tools preferred by their institutions. Will any security issues be overlooked because of the conflicting choices made by professors and administrators of higher education institutions?

Researcher's Notes

The researcher will take notes at each stage of the interview and focus group processes. The notes from the professor and student pilot interviews will help the researcher to refine and adapt the questions and facilitation process for the real interviews and student focus group. The notes taken by the researcher during the actual interviews and student focus group will act as a point of reference to assist the researcher with the issue of accuracy, triangulation, and validation. The notes themselves are part of the qualitative research process. Specific words, quotations, intonations, inflections in

participants' voices indicating hesitation or bewilderment or not knowing the answer to certain security questions, and decision not to answer certain questions will be included in the notes.

Summary

The two methods of data collection, interview and focus group, supplemented by researcher notes, should provide enough information to the researcher to answer the questions posed in this exploratory research design. Professors may provide distinctive answers pertaining to their experiences of teaching online; the students may give answers from the experiences that they suffer during their study online. Responses from these two groups should provide solid answers to the questions that drive the researcher to design and carry out this project. The responses or data collected from these two groups will be analyzed separately and the general report will be combined so that each of them will complement the other. The reason for the separate data analysis is because the two groups have had different sets of questions in which different answers were given about the online security experiences of the students and professors. The researchers notes will be of use in the coding and interpretation of the recorded data.

Methods of Data Analysis

After transcription of recorded interviews and the focus group, and preliminary analysis, detailed coding will be done using NVivo software. Patterns revealed by coding during the analysis should help the researcher to extract the required results and give meaning to the interpretations of the cybersecurity issues encountered by the two groups of participants, students and professors. The complex online security realities experienced

by the participants should be apparent from the analysis. The comparison between students' data and that collected from the professors will be minimal in that the two groups have slightly different perspectives: professors in this research design come from the position of professors; their problems are not the same as those experiences by the students. The students on the other hand approach online security phenomena as learners in a new environment. The two groups have one thing in common: the safety of their personal information as well as the safety of their personal resources such as computer hardware and software and copyright material. The researcher's notes will help the researcher to refine the data gathering method prior to starting the focus groups discussion and to guide the analysis.

The Trustworthiness of the study

Trustworthiness, validity, and the justification for the research are very critical in this study. The questions that relate to the trustworthiness, validity, and the justification of the research on online security will be addressed by the method chosen to answer the questions mentioned in the literature review. Shenton (2004) put forward a number of strategies for dealing with the issues of trustworthiness. They include credibility, reliability, transferability, and objectivity preference (confirmability).

McMillan and Schumacher (2010) described trustworthiness as a form of validity. It is important in this respect to give readers, researchers, stakeholders, or academics and non-academics some assurance that this study is valid or has a high degree of trustworthiness (Patton, 1990). The researcher will use several methods to make it trustworthy. The first strategy is using triangulation, which entails adopting several

methods when carrying out research. These include techniques such as member checking, participant reviews, and mechanical recording of data. Recorded data will help to act as backup to analysis because the researcher can always go back to make sure a particular participant meant what he or she said during the interview or focus groups discussion. The researcher can check with him or her again if this becomes important for validation purposes. The triangulation technique of participant review is essential to the proposed study. Because the number of participants is small, it will not be difficult to arrange for them to review the transcript of the interview and correct or agree with the stored information (McMillan & Schumacher, 2010). The researcher will also watch for negative or discrepant data during the recorded interview. In this way, the researcher can report on the views of the two groups of stakeholders, who may have differing opinions about online security for electronic learners. To reinforce the validity or trustworthiness question further, the researcher will use the exact views or accounts of the stakeholders recorded during the interview.

The supervisor and his team, and the participants are all part of the validation process. They will have approved and followed this project research design from the beginning to end, making sure all the necessary information is included, and unnecessary data removed. Therefore, they also contribute to trustworthiness. The researcher must be as objective as possible to collect, analyze, and present valid and reliable data to have academic credibility even if there is some probability of subjectivity in the research. The subjectivity comes from the fact that the researcher is part of this research process

(McMillan & Schumacher, 2010). The latter fact cannot be entirely avoided, but it must be mitigated.

Also, all participants will be assured of strict confidentiality in the handling of the data they supplied, and they are free to participate or refuse to participate in this research. Free individual stakeholders will have a greater reliability if they are not coerced to participate in the study. Specific data regarding the circumstances of the participants will be gathered and their profile presented: the circumstances may include the level of knowledge and skills of the participants about online attacks; what they do after their computer systems, applications, and data are corrupted or destroyed; and what issues they are worried about.

The study has two methods of triangulation. Guion, Diehl and McDonald (2011) define triangulation as a tool used in qualitative research to establish validity, a concept that means research findings must be true and certain. They categorize five types of triangulation: data, investigator, theory, methodological, and environmental. This study design uses data triangulation (comparison of findings from two types of stakeholders) and methodological triangulation (comparison of what is revealed from student interviews and the student focus group).

To contribute further to trustworthiness, the investigator will carry out member checking by sharing transcripts with participants and asking for verification or further clarification. A portion of the transcribed data will be coded by an experienced researcher to check coding reliability. Finally, the researcher will use his personal journal entries

documenting the study process and discussions with his supervisory committee about the interpretation of data.

Limitations of the Study Design

First, the time of program completion and logistics have limited the researcher's ability to carry out an overly ambitious, comprehensive and large-scale qualitative research regarding this topic. The reason is that the scope of the research and its design have been limited by the need to manage and complete the Master's in Education (M.Ed.) degree program.

Second, the researcher anticipates some problems related to the technical know-how and other barriers that may hinder the interview and the process of the focus group from being conducted successfully. This may include lack of commitment from the two groups of participants, students and professors, and other unforeseen circumstances that may prevent the two events from being carried out as expected. The set up of the pilot study is supposed to minimize some of these problems. However, obstacles such as natural disasters, power outages, and illness may not be avoided altogether. If these circumstances involve the three professors, a rescheduling of the time should help minimize this conflict. If it involves one or two students, the process will continue without rescheduling for another time.

Summary and Conclusion

This exploratory study focuses on the role played by students and professors as the main groups that use online studies in the emerging field of information and communication technology. The study examines their perceptions, awareness, and

attitudes towards cybersecurity and data integrity, which have become problematic to them and to others who use the internet for educational purposes. As institutions of higher learning rush to adopt this medium of communication and tap into the growing student market worldwide, they overlook online security to the detriment of all internet users including these institutions. This exploratory study design argues that the students and professors should be protected, while they are studying or teaching online.

The responsibility to protect the privacy of the students and professors online falls on their institutions and on students and professors themselves. The literature review has revealed that serious attacks happen undetected every day.

The stakes are much higher for these stakeholders now than they were in the early days of the internet; the study is significant in that it will explore how users learn about online security and how they can defend themselves online. The literature review reveals insufficient treatment of this topic as it relates students and professors to security and their work in an online learning environment. The collection of data follows qualitative (in-depth interview) approach and focus groups. The research questions to be answered center around the experience, knowledge, perceptions and attitudes of the students and professors, regarding their safety online.

The literature review has revealed that learners and professors are susceptible to simple and advanced online attacks; moreover, all computer systems and other software applications are not immune from hackers, who have become very sophisticated in their hacking methods. The attacks can be executed from anywhere in the world, wherever and whenever there is internet access. Besides, some of the students and professors have no

basic knowledge of the frequency, magnitude, and severity of the online attacks; others who are experts in the field of computer security take all necessary precautions and measures to protect their privacy and that of their computer systems and applications. Some institutions leave the responsibility of privacy protection to the students and professors themselves. The study design seeks to examine what stakeholders know about cybersecurity and or what knowledge and training they have received to be able to protect themselves with confidence against online attacks.

References

Abawajy, J. & Kim, T. (2010). Performance analysis of cyber security awareness delivery methods, (p. 141-148). Berlin, Heidelberg: Springer: doi: 10.1007/978-3-642-17610-4_16

Academic Partnerships. (2011). Research on the effectiveness of online learning: A compilation of research on online learning. *The Future of State Universities.* Retrieved from http://www.academicpartnerships.com/research/white-paper-research-in-online-learning.

Adams, A., & Blandford, A. (2003). Security and Online Learning: To Protect and Prohibit. In C. Ghaoui (Ed.), *Usability Evaluation of Online Learning Programs (*pp. 331-359). Hershey, PA: Information Science Publishing. doi:10.4018/978-1-59140-105-6.ch018

Adkins, A. S. (2009). Innovation in educational technology: The virtualization of K-12 and higher education. *Ambient Insight's "Learning Technology Innovation" Webinar Series hosted by Elluminate.* Retrieved from https://sas.elluminate.com/site/external/event/description?instance_id=15563

Ali, A., & Elfessi, A. (2004). Examining students' performance and attitudes towards the use of information technology in a virtual and conventional setting. *The Journal of Interactive Online Learning, 2(*3), 1-9.

Alwi, N. Y. M. (2012). *E-learning stakeholders information security vulnerability model.* (Doctoral dissertation). Cranfield University, Bedfordshire.

Anderson, T. E. (Ed.). (2008). *The theory and practice of online learning*. Athabasca, AB: Athabasca University Press.

Athabasca University. (2003). *Information technology electronic data security policy*: *Policy & procedures manual*, Office of the University Secretariat. Retrieved from http://ous.athabascau.ca/policy/computingservices/informationtechnology.htm

Attride-Stirling, J. (2001). Thematic networks: An analytic tool for qualitative research. *Qualitative Research, 1(3),* 385-405.

Balaji, M. S., & Chakrabarti, D. (2010). Student interactions in online discussion forum: Empirical research from 'Media richness theory' perspective. *Journal of Interactive Online Learning, 9*(1),1-22

Bates, T. (2010). The online higher education market in the USA. *Online learning and distance education resources. Contact North.* Retrieved from http://www.tonybates.ca/2010/02/08/the-online-higher-education-market-in-the-usa/

Bates, T. (2013). Outlook for online learning in 2013: online learning comes of age. *Contact North.* Retrieved from http://www.tonybates.ca/2013/01/06/outlook-for-online-learning-in-2013/

Belawati, T. (2006). Financial management system in open and distance learning: An example at Universitas Terbuka. *A Quarterly of the Commonwealth Educational Media Centre for Asia, 12*(1). Retrieved from http://www.cemca.org.in/ckfinder/userfiles/files/sept2006.pdf

Berge, Z. L. (1998). Barriers to online teaching in post-secondary institutions: Can policy changes fix it? *Online Journal of Distance Learning Administration 1(2).* Retrieved from http://www.westga.edu/~distance/Berge12.html

Billo, C., & Chang, W. (2004). *Cyber warfare: An analysis of the means and motivations of selected nations state.* Dartmouth College, Institute for Security Technology Studies. Retrieved from http://www.ists.dartmouth.edu/docs/execsum.pdf

Breivik, P. S., & Gee, E. G. (2006). *Higher education in the internet age: Libraries creating a strategic edge /* (Fully updated and rev. ed.). Westport, Conn.: Praeger.

Calgary Herald. (2013, January 18). Ottawa faces class-action lawsuit over lost student loan data. *Calgary Herald.* Retrieved from http://www.calgaryherald.com/news/alberta/Ottawa+with+class+action+lawsuit+lost+student+loan+data/7835242/story.html

Campbell, A. (2010). Cyber crime strategy: UK home office. Retrieved from http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf

Canada's Cyber Security Strategy. (2012). Cyber security: Cyber security matters to everyone every day. Retrieved from http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

Carstens, D. S., McCauley-Bell, P. R., Malone, L. C. & DeMara, R. F. (2004). Evaluation of the human impact of password authentication practices on information security. *Informing Science: The International Journal of an Emerging Transdiscipline*, *7*, 67-85.

Carter, E., Faircloth, J., & Fraklin, C., & Loeb, L. (2002). *Hack Proofing XML*. Elsevier Science & Technology Books. Syngress.

Caswell, T., Henson, S., Jensen, M., & Wiley, D. (2008). Open content and open educational resources: Enabling universal education. *The International Review of Research in Open and Distance Learning, 9(*1). Retrieved from http://www.irrodl.org/index.php/irrodl/article/view/469/1001

CBC News. (2013, January 11). Federal agency loses data on 538,000 Canadians. *CBC News, Canada.* Retrieved from http://www.cbc.ca/news/canada/story/2013/01/11/hard-drive-missing-student-loans.html

Chen, C., Nojiri, M. M. & Sreethawong, W. (2010). Search for the elusive Higgs boson using jet structure at LHC. Retrieved from http://arxiv.org/pdf/1006.1151.pdf

Cimons, M. (2012). Cybersecurity: Training students: CyberWatch spans all school levels. *USNews News Science.* Retrieved from http://www.usnews.com/science/articles/2012/05/29/cybersecurity--training-students.

Common Weaknesses Enumeration (2011). *A community-developed dictionary of software weakness types.* Retrieved from http://cwe.mitre.org/data/

Computer Security Institute. (2011). *Education, community and research for information security professionals.* Retrieved from http://gocsi.com/public/dbir

Cook, T., Conti, G., & Raymond, D. (2012). When good ninjas turn bad: Preventing your students from becoming the threat. *Proceedings of the 16th Colloquium for Information Systems Security Education.* Orlando, FL

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches.* Thousand Oaks, CA: Sage Publications.

CyberPatriot. (2013). Air force Association's CyberPatriot. National High School Cyber Defence Competition. Retrieved from http://www.uscyberpatriot.org/Pages/default.aspx

Dabaj, F. (2011). Analysis of communication barriers to distance education. A review study. *Online Journal of Communication and Media Technology*, *1*(1), 1-15

Davis, A. (2004). Developing an infrastructure for online learning. *Theory and practice of online learning*. Athabasca University. Retrieved from http://cde.athabascau.ca/online_book/ch4.html

Denning, D. E. (2007). Assessing the computer network operations threats of foreign countries. *Information strategy and warfare: A guide to theory and practice,* (pp. 187-210). New York, NY: Routledge.

Dorothy, D. E. (2008). The ethics of cyber conflict. *The handbook of information and computer ethics, 407.*

Dykman, C. A. & Davis, C. (2008). Online education forum: Part Two—online versus teaching conventionally. *Journal of Information Systems Education, 19(2)*

Easton, S. S. (2007). Online learning: Expectations and experiences: A comparative analysis between online and face-to-face classes in interpersonal communication. *International Journal of Learning, 12(5),* 177-186.

EDUVENTURES. (2013). Trend to blend: Thoughts from the Sloan-C Blended Learning Conference 2013. *EV Perspectives*. Retrieved from http://www.eduventures.com/ev-perspectives/

El-Khatib, K., Korba, L., Xu, Y. & Yee, G. (2003). Privacy and security in e-learning. Institute for Information Technology. *National Research Council of Canada*.

European Commission. (2013). EU cybersecurity plan to protect open internet and online freedom and opportunity – Cyber Security strategy and Proposal for a Directive. Retrieved from http://ec.europa.eu/digital-agenda/en/our-goals/pillar-iii-trust-security

Evans, K., & Reeder, F. (2010). *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters.* Center for Strategic and International Studies (CSIS). Retrieved from http://csis.org/files/publication/100720_Lewis_HumanCapital_WEB_BlkWhteVersion.pdf

Fan, S. (2011). *Web-based learning in Australian tertiary education: Insights of the end-users.* Saarbrucken, Germany: LAP Lambert Academic Publishing.

Fowler, A. & Cronau, P. (2013). Hacked! *Four Corners. ABC.* Retrieved from http://www.abc.net.au/4corners/stories/2013/05/27/3766576.htm

Gorman, S. (2013). Annual cybercrime costs are put near $100 billion. *Barron's*. Retrieved from http://online.barrons.com/article/SB40001424127880457862188096624299 0.html

Green, K. C. & Wagner, E. (2011). Online education: Where is it going? What should boards know? *Trusteeship, 19(*1*),* 24-29.

Grobler, M., Dlamini, Z., & Ngobeni, S., Labuschagne, A. (2011). Towards a cyber security aware rural community. Retrieved from http://researchspace.csir.co.za/dspace/bitstream/10204/5183/1/Grobler3_2011.pdf

Guion, A., Diehl, D. C., & McDonald, D. (2011). Triangulation: Establishing the validity of qualitative studies. Retrieved from http://edis.ifas.ufl.edu/fy394

Hathaway, O. & Crootof, R. (2012). The law of cyber-attack. Yale Law School. *Faculty scholarship series,* Paper 3852. Retrieved on from http://digitalcommons.law.yale.educ/fss_papers/3852.

Homeland Security Digital Library - HSDL. (2009). Securing homeland security through the power of innovation. *Homeland Security Digital Library Quarterly Newsletter, 1(2.).*

Hong, J., Kim, J., & Cho, J. (2009). The trend of the security research for the insider cyber threat. In *Security technology* (pp. 100-107). Springer Berlin Heidelberg. Retrieved from http://www.sersc.org/journals/IJFGCN/vol3_no2/3.pdf

Hwang, K., Fox, G. C., Jack, J. & Dongara, J. J. (2012*). Distributed and cloud computing: From parallel processing to the internet of things.* Waltham; MA: Elsevier.

Hypponen, M. (2012). Three types of online attack. TEDx talks. ideas worth spreading. Retrieved from http://www.ted.com/talks/mikko_hypponen_three_types_of_online_attack.html.

Issues Monitor. (2011). Cyber crime – A growing challenge for governments. *KPMG International Governance, 8.* KPMG International Cooperative.

International Cooperation for Assigned Names and Numbers – ICANN. (2013). DNS risk management framework working group. Retrieved from http://www.icann.org/en/groups/other/dns-risk-mgmt

Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. Congressional Research Service, Library of Congress. Retrieved from https://www.fas.org/sgp/crs/misc/RL32331.pdf

Johnson, V. R. (2005).). *Cybersecurity, Identity Theft, and the Limits of Tort Liability*. *bepress Legal Series*, 713. Retrieved from https://www.stmarytx.edu/webfiles/law/pdf/Johnsoncyber.pdf

Kennedy, J. (2011). Cyber crime goldmine—less than 1pc of money in the world is physical. *Silicon Republic.* Retrieved from http://www.siliconrepublic.com/strategy/item/20930-cyber-crime-goldmine-less

Kim, K. & Bonk, C. J. (2006). Future of online learning in higher education: The survey says… *Educause Quarterly, 4.*

Kingkade, T. (2013). MOOC skepticism persists among university presidents despite rapid growth in online courses in 2012. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/2012/11/26/moocs-skepticism_n_2191314.html

Kovacs, P., Markham, M., &Sweeting, R. (2004). Cyber-incident risk in Canada and the role of insurance. *ICLR Research Paper Series*, *38*. Retrieved from http://www.iclr.org/images/Cyber-Incident_Risk_in_Canada_and_the_Role_of_Insurance.pdf

Kovacs, G. (2012). Tracking the trackers. *TEDx talks. Ideas worth spreading*. Retrieved from http://www.ted.com/talks/gary_kovacs_tracking_the_trackers.html

Lewandowski, J. O. (2005). Creating a culture of technical caution: Addressing the issues of security, privacy protection and the ethical use of technology. *Proceedings of the 33rd Annual ACM SIGUCCS Fall Conference,* 184-187.

Manson, D. (2013). LAUSD partnership exposes students to cybersecurity careers. *Community Partners*. *College of Business and Administration*. Retrieved from https://cba.csupomona.edu/cba/news/cyber_patriot.aspx

McKay, J. (2012). Cybersecurity curriculum on tap for University of Maryland students: Training & Education. *Strategy & Leadership in Uncertain Times, EMERGENCY Management.* Retrieved from http://www.emergencymgmt.com/training/Cybersecurity-Curriculum-University-Maryland-Students.html

McMillan, J. H., & Schumacher, S. (2010*). Research in education: Evidence-based inquiry* (7th ed.). Boston: Pearson.

Meyer, K. (2008). If higher education is a right, and distance education is the answer, then who will pay? Sloan Consortium, *Journal of Asynchronous Learning Networks,* 12 (1).

Nagel, D. (2010). The future of e-learning is more growth. *Education, 34,* 54.

Nance, N., Hay, B., Dodge, R. Seazzu, A. & Burd, S. (2009). Virtual laboratory environments: Methodologies for educating cybersecurity researchers. *Methodology Innovation Online, 4*.(3), 3-14.

National Institute for Cyber-security Education. (2011). Building a digital nation. Retrieved from http://csrc.nist.gov/nice/documents/nicestratplan/Draft_NICE-Strategic-Plan_Aug2011.pdf

National Vulnerability Database. (2011). Automating vulnerability management, security measurement, and compliance checking. National Institute of Standards and Technology. Retrieved from http://nvd.nist.gov/cwe.cfm

New Media Consortium. (2007). The horizon report 2007 edition. Retrieved from http://www.nmc.org/pdf/2007_Horizon_Report.pdf

North, M. M., George, R., & North, S. M. (2006). Computer security and ethics awareness in university environments: A challenge for management of information systems. *Proceedings of the 44th Annual Southeast Regional Conference (ACM-SE 44). New York, NY: ACM*, 434-439.

Office of Information Technologies – OIT. (2012). Safeguarding sensitive information. OIT Annual Report. University of Notre Dame: Retrieved from http://oit.nd.edu/about-oit/oit-annual-report/

Onwuegbuzie, A. J., & Leech, N. L. (2007). A call for qualitative power analyses. *Quality & Quantity, 41(*1), 105-121. Retrieved from http://users.polisci.wisc.edu/schatzberg/ps816/onwuegbuzie2007.pdf

Open Web Application Security Project. (2012). Global connector election edition. Retrieved from http://owasp.blogspot.ca/

Orrey, K. (2010*). Cyber attack: Exploiting the user–There are so many ways! MSc. Computer Security and Forensics. Master's Thesis Report* (Unpublished master's thesis). Faculty of Creative Arts, Technologies and Sciences (CATS). University of Bedfordshire, Bedfordshire. Retrieved from http://www.vulnerabilityassessment.co.uk/education/Thesis.pdf

Patton, M. Q. (1990). Qualitative evaluation and research methods (3rd ed). Thousand Oaks, California: Sage Publications.

Potanos, T. F. (2012). Dueling values: The class of cyber suicide speech and the First Amendment. *Chi –Kent I. Rev., 87, 669.*

Polycentric. (2013). Alum gives to cybersecurity program. Pomona, CA: California State Polytechnic University, Pomona. Retrieved from http://polycentric.csupomona.edu/news_stories/2013/06/alum-gives-to-cybersecurity.html

Power, M. (2008). The emergence of a blended online learning environment. *MERLOT Journal of Online Learning and Teaching, 4(*4) 503-514. Retrieved from http://jolt.merlot.org/vol4no4/power_1208.pdf

Queen's University. (2005). Queen's University computer user code of ethics. University Secretariat. Retrieved from http://www.queensu.ca/secretariat/policies/senateandtrustees/computerethics.html

Rennie, S. (2013*). Government faces class-action lawsuits over student loan borrowers' lost data.* The Globe And Mail. The Canadian Press. Retrieved from http://www.theglobeandmail.com/news/politics/government-faces-class-action-lawsuits-over-student-loan-borrowers-lost-data/article7492261/

Rickard, W. (2010). The Efficacy (and inevitability) of online learning in higher education. *Pearson Learning Solutions.* Retrieved from http://chronicle.com/items/biz/pdf/Pearson_WP_EfficacyOfOnlineLearning.pdf

Romiszowski, A. (2004). How's the e-learning baby? Factors leading to success or failure of an educational technology innovation. *Educational Technology, 44*(1), 5-27.

Royal Canadian Mounted Police – RCMP. (2013). Internet security. Retrieved from http://www.rcmp-grc.gc.ca/qc/pub/cybercrime/cybercrime-eng.htm

Rubin, A. (2012). All your devices can be hacked. *TEDx talks. Ideas worth spreading*. Retrieved from http://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked.html

Rudestam, K. E., & Schoenholtz-Read, J. (2010*). Handbook of online learning* (2nd ed.). Thousands Oak, California: Sage Publications.

Schjølberg, S., & Ghernaouti-Hélie, S. (2009). A global protocol on cybersecurity and cybercrime. *Cybercrimelaw.net.* Retrieved from http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf

Sewel, J. P., Frith, K. H. & Colvin, M. M. (2010). Online assessment strategies: A primer. *MERLOT Journal of Online Learning and Teaching, 8*(1).

Shaeffer, B. S., Chan, H., Chan, H. & Ogulnick, S. (2009). Cyber crime and cyber security: A white paper for franchisors, licensors, and others. Riverwoods, IL: Wolters Kluwer, Law & Business. Retrieved from http://business.cch.com/franlaw/cybercrime_whitepaper.pdf

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for information, 22*(2), 63-75. Retrieved from http://iospress.metapress.com/content/3ccttm2g59cklapx/

Stacey, E. (2009). Research into cyberbullying: Student perspectives on cybersafe learning environments. *Informatics in Education-An International Journal, 8*(1), 115-130.

Stake, R. E. (2010). *Qualitative research. Studying how things work.* New York, NY: The Guilford Press.

Stange, C. (2011). Privacy concern and student engagement in the virtual classroom (Unpublished master's thesis). University of Victoria. Retrieved from http://distance.uvic.ca/pdfs/Privacy-Concerns-and-Student-Engagement.pdf

Stallings, W., & Brown, L. (2012*). Computer security: Principles and practice* (2nd ed.). Upper Saddle River, New Jersey: Pearson Education.

Stuttard, D., & Pinto, M. (2011*). Web application hacker's handbook: Finding and exploiting security flaws* (2nd ed.). Indianapolis, Indiana: Wiley Publishing.

Sullivan, B. & Liu, V. (2012). *Web application security: A beginner's guide*. New York, N. Y.: McGraw-Hill.

Tallent-Runnels, M. K., Thomas, J. A., Lan, W. Y., Copper, S., Ahem, T. C., Shaw, S. M. & Liu, X. (2006). Teaching courses online: A review of the research. *Review of Educational Research Spring, 7, 693-135*. Retrieved from http://rer.sagepub.com/content/76/1/93.short

Thabane, L., Ma, J., Chu, R., Cheng, J., Ismaila, A., Rios, L., ... & Goldsmith, C. (2010). A tutorial on pilot studies: the what, why and how. *BMC medical research methodology*, *10*(1), 1.

The University of Texas at Austin. (2011). Evaluate programs: Focus group. *Instructional Assessment Resources (IaR).* Retrieved from http://www.utexas.edu/academic/ctl/assessment/iar/

University of Maryland. (2013). Advanced cybersecurity experience for students (ACES): A new model for cybersecurity education. Retrieved 26, 7, 2013, from http://www.honors.umd.edu/ACES-facts.pdf

U.S. Department of Defense. (2011). The cyber domain: Security and operations. Retrieved from http://www.defense.gov/home/features/2013/0713_cyberdomain/

Van Cleef, A., Pieters, W., & Wieringa, R. J. (2009). Security implications of virtualization: A literature study. In *Computational Science and Engineering, 2009. CSE'09. International Conference on* (Vol. 3, pp. 353-358). IEEE

Velte, A. T., Velte, T.J. & Eisenperter, R. (2010). *Cloud computing: A practical Approach*. New York, NY: McGraw-Hill Companies.

Wagner, N., Hassanein, K., & Head, M. (2008). Who is responsible for e-learning success in higher education? A stakeholders' analysis. *Journal of Educational Technology & Society, 11*(3), 26-36.

Willems, C. & Meinel, C. (2012). Online assessment for hands-on cyber security training in a virtual lab. *Internet Technologies and Systems Group*, Hasso Plattner Institute, University of Potsdam, Potsdam.

Willard, N. E. (2007). *Cyberbullying and cyberthreats (Book and CD): Responding to the challenge of online social aggression, threats and distress*. Champaign, IL: Research Press.

Zhang, D. & Nunamaker, J. F. (2003). Powering e-learning in the new millennium: An overview of e-learning and enabling technology. *Information System Frontiers, 5*(2), 207-218.

Appendix A. Students' Interview Questions Guide

This appendix describes the guidelines for the online interview.

The participants would have received a username and password in an email sent in advance of this interview. After a participant student logs in, the researcher will thank him or her and explains to him or her the purpose of the interview, the protocols of the procedure, and the time allocated for this period.

At the end of the interview, the researcher will ask the participants to ask any question or make any useful comments about their participation. Specifically, the researcher will ask the participants whether their views have changed, whether they have learnt something new about online security, and if so whether they will change their online behavior.

Engagement questions

1. What course or courses have you taken online?
2. How long did the course (s) lasts? Describe your feelings and experience about this online course (s)?
3. Why did you take this course or these courses online?

Exploration questions

1. What do you know about online security?
2. What privacy or security issues have you encountered while taking courses online?
3. What steps did you take to protect yourself and your data while studying online?

4. How do you learn about online security? Describe any specific steps. (Prompts: Did your professor or professors provide you with any guidance or recommendations concerning online privacy or security? What did you learn from your friends/colleagues about how to protect yourself and your computer system and other software applications from online intruders or dangerous malware? Your own research or reading? Your own experience? Courses or workshops?)
5. How did you address the issues in questions g? (Repeat question g to the participants)
6. How can you tell that your computer system or data have been or have not been compromised or corrupted?
7. How do you feel about the computer or online security protection provided by your institution (College or University)?
8. What is the roll of your institution with regards to online privacy protection of students' data, computer systems and software applications? Probe: Explain what you mean by that.
9. Have you communicated or shared any educational ideas with your colleagues and friends using social media? Describe the specific media you have used? How do you feel about its security settings?

Exit questions

1. Is there any specific online security issue (s) you would like to be discussed? (Only one question will be selected or accepted on the basis of its importance if there are many).

This is the end of the questions for the online interview. Thank you for your participation.

Appendix B. Questions for Student Participants in the Focus Group

The following are the questions for students in the focus group.

First, the researcher will need a competent assistant in running the focus groups: the work of taking notes, recording statements from the participants and controlling the whole process needs an extra helper, who has signed a confidentiality agreement with the researcher and his supervisory team: the purpose of the agreement is to assure the participants that such a person will not disclose any of their information to any other party.

Unless a participant expects a very serious emergency (e.g, a child in hospital) no smartphones are allowed to go off during the discussion. Participants will be gently but firmly reminded to switch their cell phones off; cell phones can be very distracting to the rest of the group. Equally, participants will be requested not to check messages or text anyone during the discussions.

Some of the assumptions about this group include their need to participate and contribute ideas to the important topic of studying online, while knowing how to protect one's privacy; they will also contribute any historical attack incidents that they have suffered and discuss the circumstances they were in at the time of the attack, what actions they took to resolve the problem, and what lessons they learned from the incidents.

Below are the questions taken from the research questions outlined in Chapter 1. The time is 90 minutes. Each participant has a maximum of 5 minutes to answer the questions. There are a total of 5 questions that the participants will discuss in a frank and

friendly atmosphere. It is done online and will be recorded. This fact must be clear to the participants, who have the freedom whether or not to participate.

Questions for the Students' Focus Group Discussion

Question One: Online Security Problems:

Describe any security breach that you have encountered while using the internet for educational purposes.

1. Probe: What were you doing at the time?
2. Probe: What software were you using?
3. Probe: When did the problem occur?
4. Probe: How did you feel about the security breach / was anything valuable lost?

Question Two: Knowledge as a Source of Defence

What do you know about online security?

1. Probe: Tell me more about any methods used by intruders or hackers to gain unauthorized access to your computer system, your computer applications and personal data?
2. Probe: To what extend do hackers interfere with online learning and free discussions in online discussion boards for students?
3. Probe: Describe some of the barriers or factors that contribute to online identity theft.

4. Probe: Does anyone know any serious threats to you as students when you are studying online? Talk about three major threats. The question is directed to the whole group, but the current speaker may answer it too.

Question Three: Protection Mechanism

What steps do you as a student take to protect yourself and your assets (laptops, software, and data) against online attacks?

1. Probe: Define any effective mechanisms, methods, or software that you have used or are using now to protect yourself and your computer applications while you are studying online?
2. Probe: What procedures would you follow after an attack incident?
3. Probe: Describe any privacy protection recommendations or training you have received from your professors and institutions.
4. Probe: Describe the reasons you use backups? Where do you backup your data and computer applications?

Questions Four: The Gap between Knowledge and Online Security Practice

What bothers you the most about the gap between what you know or do not know about cybersecurity and what you practice in your online studies?

1. Probe: What are some of the examples of the gaps that you think exist between knowledge and good practice?
2. Probe: Can anyone describe why there are gaps between knowledge and practice with respect to privacy online?

Question Five: The Methods Students Use to Learn about Cybersecurity

How do you learn about cybersecurity?

1. Probe: Describe any specific methods that you take to learn about online privacy. Under what circumstances do you decided to learn about online security?
2. Probe: Where do you go to seek help to learn about cybersecurity? What resources or ideas do you use to increase your knowledge?
3. Probe: Describe to me when you started learning about online security.

This is the end of our focus group discussion. Is there any online security issue (s) you would like us to discuss? Only one or two questions will be allowed. Thank you for your participation.

Appendix C. Questions for Online Interview with Professors

The following are the questions for the online interview with professors.

The questions are different from the ones given to the students. The reason is that professors have a different approach to the online privacy issue: They are the facilitators of online learning. Some of the professors may know a lot about online security because they teach computer security courses, which are closely related to this topic. Other professors may know nothing or very little about cybersecurity because it is not their field of expertise. The latter may rely on their institutions' IT department for security issues, or they may receive cursory security training in form of one-to-two week's workshop or training from their institution. This is not enough for them to help themselves or their students. These professors then suffer the same fate as the students who do not know about cybersecurity.

The interview questions asked here are both for expert and non-expert professors, regarding security and privacy in an online learning environment. The time is 60 minutes, and 10 questions. The number of professors is three; the interview is recorded, but highly confidential. They should have been aware of this. The participation is voluntary.

The researcher is interested in the answers to the questions elicited from the expert and non-expert professors as described here. The research design is not a comparison between those who know and those who do not know.

Questions for the Professors' Online Interview

Engagement questions

1. What course or courses have you taught online?

2. How long did the course (s) last?
3. Describe your experience in teaching this course (s) online, in terms of security and authentication controls?

Exploration questions

1. Describe any computer security training that you might have received prior to teaching online? If none, what do you know about online security?
2. Which information security (computer security) membership do you hold? Membership in an organization or association such as the Information Systems Security Association (ISSA) indicates a level of seriousness and computer security sophistication. If you do not belong to any of these organizations, how do you protect yourself and your students in online learning environment?
3. What privacy or security issues have you encountered while teaching courses online? You may describe three major security attacks or issues you have encountered (possible more if need be).
4. What online computer security advice would you give to your students to stay safe, especially those who have no clue about cybersecurity?
5. Describe the gap or gaps between your knowledge and your actual practice, regarding online security for you and your students.
6. Keeping up to date with the latest cybersecurity breaches: How do you keep yourself and your students up to date regarding the latest and deadliest attacks on online privacy?

7. What computer security policies regarding software choices from your institutions do you agree or disagree with, particularly those connected with the course management systems (CMS) or leaning management systems (LMS)?

Exit questions

1. Is there any specific online security question (s) you would like to ask?

This is the end of the questions for the online interview. Thank you for your participation.

Appendix D. Letter of Information and Consent

Letter of Information and Consent for Participation in Research Interview or Online Focus Group

313-1400 Lepage Avenue
Ottawa, Ontario, K1Z 8N5
September 27, 2013
Dear Prospective Research Participant:

I am a graduate student in the Faculty of Education, Queen's University, Kingston, Ontario. I am studying for a degree of Master's in Education, under the supervision of Dr. William Egnatoff. I am in the process of investigating the role of stakeholders in creating and providing a secure online learning environment for electronic learners. I hope to help raise awareness about this crucial topic and to contribute to the prevention of cyber attacks that can cause serious damage and disaster to the privacy of the students, the professors, and the networks of institutions of higher learning in which they belong.

I am, therefore, writing to request your approval to participate in this study, during which time I will conduct one interview with you at a time that is convenient to you. The interview will take approximately 60 minutes and will be conducted online. You may participate from a convenient location of your choice, provided only that it is free of distractions. The questions will concentrate on your experiences and perspectives towards online security in relation to the safety of your data, computer systems, and software applications, as well as your safety in an online learning environment. [for student participants: In addition, I am requesting your participation at a later date in an

online focus group with the other student participants. The focus group discussion will last approximately one and one-half hours.]

Your identity as participant will be protected to the extent possible. No personal information will identify you or the institution to which you are affiliated. It is free of risk, and you are free to participate to answer any questions you think will contribute to the safety of the online learning. If at any point in time during the interview you feel that you cannot answer the question(s) posed, you may refuse to answer. Your decision will be respected. If you wish to withdraw your participation in the research process, you will be free to do so. You are under no obligation to participate. However, the information you give during the interview will make cyber learning a safer experience for many students who may decide to take online courses now or in the future. If you request that the data you give during interview be removed, it will be done promptly.

The data will be kept in a computer resource area in a locked location and will not contain any of your identification. The study is voluntary and may be withdrawn at any time. The data will be securely locked and will be confidentially protected.

The data in this study may be used in journal articles, magazines or research citations. But your identity will not be made known to publication.

If you have any questions about this research or thesis, contact me at (613) 421-7652; address: Saturlino Lohure Leandro, 313-1400 Lepage Avenue, Ottawa, Ontario, K1Z 8N5.

My email is 2sl15@queensu.ca, and my Supervisor's email is egnatoff@queensu.ca.

If you are willing to participate in this research, please email me to indicate your consent. At the beginning of the interview [for students: and the focus group session], I will again ask for your consent, reminding you of the conditions and addressing any questions. Your indication of consent will be included in the recording of the session[s].

If you have any concerns about the research, contact the Research Ethics Board and the Dean of the Faculty of Education at (613) 533-6210 and the Chair of the Queen's University General Research Ethics Board at (613) 533-6081.

Sincerely,
Saturlino Leandro