Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2010 Proceedings

Americas Conference on Information Systems (AMCIS)

8-2010

Information Security Practices in Latin America: The case of Bolivia

Indira R. Guzman
TUI University, iguzman@tuiu.edu

Santos M. Galvez
TUI University, sgalvez@tuiu.edu

Jeffrey M. Stanton
Syracuse University, jmstanto@syr.edu

Kathryn R. Stam
SUNY-Institute of Technology

Information Security Practices in Latin America: The case of Bolivia

Indira R. Guzman
TUI University
iguzman@tuiu.edu

Santos M. Galvez
TUI University
sgalvez@tuiu.edu

Jeffrey M. Stanton
Syracuse University
jmstanto@syr.edu

Kathryn R. Stam
SUNY-Institute of Technology
e-mail address

ABSTRACT (REQUIRED)

In this paper, we present a social/behavioral study of individual information security practices of internet users in Latin America, specifically presenting the case of Bolivia. The research model uses social cognitive theory in order to explain the individual cognitive factors that influence information security behavior. The model includes individuals' beliefs about their abilities to competently use computer information security tools and information security awareness in the determination of effective information security practices. The operationalization of constructs that are part of our research model, such as information security practice as the dependent variable, self-efficacy and information security awareness as independent variables , are presented both in Spanish and English. In this study, we offer the analysis of a survey of 255 Internet users from Bolivia who replied to our survey and provided responses about their information security behavior. A discussion about information security awareness and practices is presented.

Keywords (Required)

Social Cognitive Theory; Information Security Behavior; Security Awareness and Practice

INTRODUCTION

With the emergence of the TCP/IP internet protocol worldwide in 1973, every country in the world, including in Latin America, was "opened" to the Internet . Brazil and Mexico are listed within the top 15 countries with highest numbers of Internet users[1]. As the Internet has grown, individuals, organizations, and these societies began to explore the richness and all the potential that the new service has to offer, and have been using it in all kinds of activities ever since. Opening the world to the Internet was a great opportunity for people and business; however, it is also an opportunity for thieves and hackers to get access to the information in organizations in an unauthorized way.

According to recent study by McAfee the cost of hacking are estimated to cost over 1 trillion globally (Mills, 2009). For instance, in cases where stolen IDs and passwords were used, the loss per incident the average loss per incident was $1.5 million (Wilson, 2006); Wilson (2006 also states that a recent survey by the Yankee Group indicates that more than half of companies rate their Internet downtime costs at more than $1,000 per hour; Finally, a study published in 2004 by the Aberdeen Group found that the cost of Internet-based business disruptions was about $2 million per incident. These figures are just the tip of the iceberg in representing the costs associated with the intentional destruction of computer-related activities.

There is a wide variety of information security risks such as viruses, worms, denial-of-service attacks, spoofing, stolen passwords, social engineering, software exploitation, trojan horses, and authority and authorization violations that can have a negative impact on the regular operations of an organization (Chen, Shaw & Yang, 2006). As security threats have grown, the need to protect organizational data has became a corporate crucial need. Although some of these attacks can be originated

[1] http://www.internetworldstats.com/top20.htm

externally, most of them are directly or indirectly originated by internal employees (Dhillon & Backhouse, 2000). For example, the most dangerous method and perhaps the easiest way of obtaining information is social engineering. Arief and Besnard (2005) refer to this as "weaknesses in wetware" which they refer to as human users. This kind of social engineering takes advantage of a basic human impulse toward helping other people, what psychologists and sociologists call prosocial behavior (Stanton & Stam, 2006). Many times, the problem is not the technology, but the users who use it. It is therefore very important to have users who are proficient in the practice of information security behaviors.

In this paper, we try to understand the factors that influence security practices in countries of Latin America, taking the case of Bolivian users. The situation of information security in Latin America is as critical as everywhere. According to a survey conducted by the Yankee Group, which interviewed 225 information technology executives in companies located in Mexico, Brazil, and Colombia,and reported by UniversiaKnowledge@Wharton (2008), more than 80% of those companies use a system of simple passwords for protecting data about the identity of their own users and only large companies use ID authentication tools such as digital certificates, tokens, and smart cards. They concluded that companies in Latin America are therefore highly vulnerable to the theft of information and that Latin American countries must improve their data protection policies, especially those that involve accessing critical information.

The purpose of this study is to evaluate the individual's cognitive factors that influence information security behavior based on Social Cognitive Theory (Bandura, 1977) in a Latin American environment which is Bolivia. This study addresses the following research questions:

- How does information security self-efficacy influence information security behavior?
- How does security awareness affect information security behavior?
- Are there significant differences in information security behavior by education, gender, IT career, computer use frequency, and Internet use frequency?

Our initial research model is presented in Figure 1.

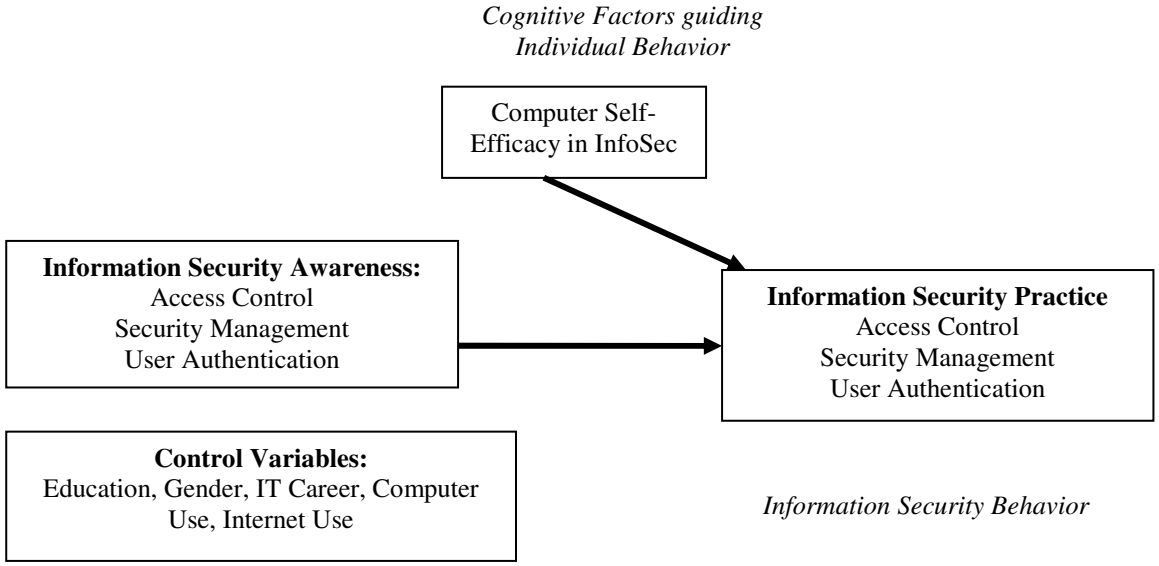

Figure 1. Research Model of Information Security Behavior

LITERATURE REVIEW

Individuals choose the environments in which they exist and are influenced by those environments. Behavior is affected by environment, which in turn are affected by behavior. Finally, behavior is influenced by personal factors of the individual, and in turn, behavior affects those same factors (Compeau & Higgins, 1995). According to Social Cognitive Theory (SCT), an individual's behavior is uniquely and reciprocally determined by each of these three factors: environmental influences such as social pressures or unique situational characteristics, cognitive and other personal factors including personality and demographic characteristics and finally, behavior (Compeau & Higgins, 1995, p.190).

According to Bandura (2002), SCT adopts agentic perspective. There are three modes of agency very well differentiated by the theory. One of them is personal agency which is implemented individually. Proxy agency is when people influence others to act on their behalf with the purpose of securing desired outcomes. Collective agency is when people exercise through group of actions. However, in this study, we focus on personal agency or individualism within the information security context. In fact, SCT has many dimensions, but in this research we are concerned with the role of cognitive factors in individual behavior, similarly to Compeau and Higgins (1995) but applied to information security context. In the paragraphs below, we present the descriptions of the dependent and independent variables of our research model.

ISP - Information Security Practice

In the information security business, there are a number of different security models proposed by professionals and organizations (Berghel, 2007). These models such as time-based security, the principle of least privilege, defense in depth, baseline security, perimeter hardening, intrusion detection, and intrusion prevention, are trying to minimize real or potential vulnerabilities and threats. The main difference between these models is the strategyused against vulnerabilities and threats, for example, time-based security (TBS) uses time as the primary measure of risk. The safety margin increases with advance warning, so as long as the advance warning exceeds the sum of the detection and response times, the information is protected. On the other hand, the principle of least privilege (POLP) relies on controls. This strategy varies inversely with the degree of control given to the application or user. Currently, there are different well-known organizations that promote specific security standards, such as the Control Objectives for Information and related Technology (COBIT), the Federal Information System Controls Audit Manual (FISCAM), the Certified Information Systems Auditors (CISA), the BSI 7799/ISO 17799/ISO 27001 standards for best practices. These standards map to government legislation or mandates such as the Health Insurance Portability and Accountability (HIPAA) (Berghel, 2007). The Information Security Organization (ISO) standards take the form of guidance and recommendations intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used (Veiga and Eloff, 2007). The ISO/IEC 27000 series is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799:2005 and then renumbered ISO/IEC 27002:2005. As stated by Veiga and Eloff (2007), ISO 17799 has gradually gained recognition as an essential standard for information security where ISO27001 (2005) is regarded as part two of ISO/IEC 17799 and proposes an approach of continuous improvement through a process of establishing, implementing, operating, monitoring, reviewing, maintaining and improving the organization's information security management (ISO, 2005; IEC, 2005). Since these security policies should be implemented within organizations, employees who follow them are actually the ones who effectively perform security practices. Ma and Pearson (2005) empirically validated seven of the ten constructs from the guidelines and practices within the most accepted and security standards by information technology professionals: ISO/IEC 17799: 2005 and BS 7799.

ISA - Information Security Awareness

According to many researchers such as Goodhue and Straub (1991); Straub and Welke (1998); Dhillon and Backhouse (2001); and Hu, Hart and Cooke (2006), information security is a socio-technological problem that requires thorough understanding of the weakest link in the defense against security threats: human behavior and attitudes about using these security technologies. The Department of Trade and Industry's 2004 Information Security Breaches Survey reports that humans are the weakest link in the chain of security control (Chen et al., 2006). Therefore, one of the preventive measures suggested by Timms, Potter and Beard (2004) was to create a security-aware culture which will have the mission of educating staff about different security risks and their responsibilities. Within the IS literature, the concept of awareness has been defined for example as "technology awareness" by Deniv and Hu (2007), as "users raised consciousness of and interest in knowing about technological issues and strategies to deal with them" (p. 391). For example, in a document of the National Institute of Standards and Technology, Lisa Lindholm defined security awareness as "an individual responsibility and sufficient understanding to comply with policies". She also indicated that security awareness is the best ROI for information security programs. According to Siponen (2000), ISA is used to refer to a state where individuals in an organization are aware of their security mission, as well as ideally being devoted to it. Information security awareness is as important as the security techniques or procedures, but the processes can be misused, misinterpreted or not used by individuals and in that way losing their real efficacy (e.g. Hoffer and Straub, 1989; Goodhue and Straub, 1989; Ceraolo, 1996; Straub, 1990; Straub and Welke, 1998). Finally, based on a literature review, Chen et al. (2006) defines ISA as an attention to security when individuals recognize IT security concerns and respond accordingly. These definitions do not imply only being informed about security issues, but actually being responsive to them, which therefore can be considered as a behavioral factor. It is important to mention that this definition also implies cognitive behavior. The increase of security awareness should minimize individual's related faults toward security threats and increase the efficiency of the security techniques and procedures

against security threats in an organization. For this study, therefore, we define ISA as users' increased consciousness of knowledge about security issues and the strategies to deal with them. ISA is one of the information security behaviors.

In order to operationalize this variable, we found three ways of measuring awareness in the IS literature: One from Dinev and Hu (2007), another from Chen et al. (2006) and one from Ryan (2006). We propose to use the approach of Ryan (2006) because it is more explicitly directed at information security. Following the literature, information security awareness is the basis of information security behavior, thus it is hypothesized that the higher the information security awareness, the higher the information security practices.

Bandura stated that the major cognitive forces guiding behavior are outcomes and self-efficacy. Outcomes-oriented individuals usually assume behaviors they believe will end up in valued outcomes. Self-efficacy influences choices about which behaviors to undertake (Compeau & Higgins, 1995).

Cognitive forces: Self Efficacy in Information Security (InfoSec)

According to Bandura (1977), self-efficacy is the individual perception or belief that one has the capability to perform a particular behavior and has sufficient skills to perform given tasks (Compeau & Higgins, 1995; Ryan, 2006). Compeau and Higgins (1995) developed and validated a construct to understand the impact of self-efficacy on individual reactions to computing technology, and it is named 'computer self efficacy' (CSE). The authors initially developed a theoretical model based on social cognitive theory (Bandura, 1986) that included the new measure of CSE. Then, they tested their model in a sample of 1020 knowledge workers in Canada, concluding that self-efficacy plays an important role in shaping individuals' feelings and behaviors towards computer use. Individuals with high self-efficacy use computers more, resulting in more enjoyment from their use, and experience less computer anxiety (Compeau & Higgins, 1995). Affect and anxiety also had a significant impact on computer use. The authors presented a follow-up study of the one published in 1995. They tested a subset of the model tested in the 1995 paper but used longitudinal data gathered from 394 end users over a one-year interval. The results confirmed that both self-efficacy and outcome expectations impact an individual's affective and behavior reactions to information technology. This later study used the scales from the earlier paper and confirmed reliability of the instrument becoming the basis for our study. The authors conclude that both self-efficacy and outcome expectations impact on an individual's affective and behavioral reactions to IT. Self-efficacy beliefs regulate human functioning through cognitive, motivational, affective and decisional processes (Bandura, 2002).

Socio Cognitive Theory has proven to be a powerful mechanism for explaining, predicting, and governing behavior and has been broadly used by researchers. For example, Havelka (2003), used data from students enrolled in an MIS course at a large Midwestern university (approximately 15,000 students) to test software self-efficacy and computer anxiety among students with different demographic predictors such as academic majors, years of experience using computers, and amounts of computer coursework, etc. The author concluded that students from different business majors had different levels of self-efficacy, and a negative relationship between software self-efficacy and computer anxiety. Other researchers, such as Hayashi, et al. (2004) conducted a field experiment to test a proposed integrative research model. The model is based on a combination of the CSE, the technology acceptance model (TAM) , Expectation-Confirmation model (ECM) and end-user computing theories. It was used to assess the intention of online learners who continued using the e-learning system as a vehicle to assimilate IT skills. La Rose and Eastin (2004) proposed and tested a new model of media attendance based on SCT. The present media usage as an explicit media consumption behavior (specifically, the use of the Internet) is determined by the anticipated outcomes that go after that consumption. In another study, SCT has helped to explain physical activity behavior among college students (Suminski & Petosa, 2006). The authors found that the Web has been shown to be a good method for bringing behavior-change programs because of its low cost and popularity among large numbers of people. Thus, it is hypothesized that the higher the individual's computer self-efficacy in information security, the higher the information security practice.

METHODOLOGY

Bolivia is a country located in the center of South America with close to 11 million inhabitants. According to the International Telecommunication Union (ITU), it has about 34,000 broadband Internet subscribers as of Nov.26/08, only 0.4% of the population[2]. Culturally, many Latin American Countries have similar values and cultural beliefs. Bolivia is one of the poorest countries but has comparable political, economic, and resource struggles as its neighbors. Therefore, we think that learning about the Bolivian case is a good starting point for understanding security behavior in Latin America. Our

[2] http://www.internetworldstats.com/sa/bo.htm

convenience sample consisted of 260 participants who were contacted through an Information Auditing class where one of our authors was teaching. The students were asked to fill out the online survey and request that their family and friends complete the survey as well. We collected a total of 255 usable responses with 176 male participants (70%) and 77 female participants (30%). The participants filled out the online survey developed with Google forms[3]. They reported that they use a computer frequently, with 89% indicating that they use the computer daily and the rest either weekly (10%) or monthly (only 1%). They also use the Internet frequently: 83% indicated that they use the Internet daily and the rest either weekly (15%) or monthly (only 2%). A large percentage (81%) of our participants indicated that they have Internet access at home. In terms of education, 40% of our participants completed high school, 46% obtained a Bachelor degree, 9% completed some graduate certification, and 6% completed a Masters degree. Finally, 110 of our participants (44%) indicated that they are pursuing or working in an information technology (IT) related career and 142 of our participants (56%) indicated that they are not pursuing or working in an IT career.

The scales used to measure information security practice, information security awareness, and individual self-efficacy in information security and were adapted from Ryan (2006) and Compeau & Higgins (1995), and then translated from English to Spanish. Table 1 provides titles, definitions, and items in both languages, as well as factor loadings and the reliabilities of the scales. It is important to mention that the scales related to encryption and physical security were eliminated due to low factor loadings, possibly due to unclear translation. Table 2 has the means, standard deviation, and correlation of the variables.

Variable	Code	Spanish	English	Factor Loading	Reliability
(With respect to information technology and its security, I am aware…) Security Awareness – Access Control	SA03TA	Software Firewall puede bloquear los ataques de red	Firewall software can block network attacks (+)	.728	.846
	SA09TA	Como usuario, mi conocimiento de las amenazas al ordenador desempeña un papel significativo	As a user, my knowledge of computer threats plays a significant role (+)	.783	
	SA12TA	Soy consciente de la repercusión que puede tener un virus en un sistema informático.	Of the impact that a virus can have on a computer system (+)	.812	
	SA13TA	Soy consciente del impacto de los ataques de redes que pueden tener en un sistema informático	Of the impact network attacks can have on a computer system (+)	.824	
	SA14TA	Soy consciente de la vulnerabilidad compartida con dispositivos como archivos, discos, impresoras.	Of vulnerability with shared devices such as files, drives, or printers (+)	.789	
Security Awareness – Security Management	SA02TS	Software antivirus requiere actualizaciones frecuentes	Virus protection software requires frequent updates (+)	.803	.681
	SA06TS	Política de Protección de virus requiere el uso de software y las actualizaciones disponibles	Virus Protection Policy requires use of available software and updates (+)	.799	
	SA16TS	El software requiere decisiones y actualizaciones periódicas.	Software requires periodic decisions and updates (+)	.747	
Security Awareness – User Authentication	SA05TU	Políticas de uso aceptable sugieren mantener las contraseñas fuertemente protegidos	Acceptable Use Policy strongly suggests keeping passwords safeguarded (+)	.827	.681
	SA07TU	Política de Uso Aceptable dicta que redes de acceso con cable e inalámbricas requieren Un usuario-ID y contraseña	Acceptable Use Policy dictates that wired and wireless network access requires a user-id and password (+)	.783	
	SA11TU	Tener una contraseña secreta es fundamental	Password secrecy is fundamental (+)	.752	
Computer Self Efficacy (In your opinion, could you install and set-up security	CSE03	Si tuviera sólo los manuales de referencias.	If I had only manuals for reference?	.765	.818
	CSE04	Si hubiera visto a otra persona utilizarlo antes de intentar yo mismo	If I had seen someone else using it before trying it myself?	.765	
	CSE06	Si alguien me hubiera ayudado a empezar	If someone else had helped me get started?	.734	

[3] http://docs.google.com/support/bin/answer.py?hl=en&answer=87809

software…)	CSE07	Si tuviera la infraestructura que facilite la asistencia.	If I had just the built-in help facility for assistance?	.790	
	CSE09	yo hubiera utilizado antes aplicaciones similares para obtener el mismo objetivo	If I had used similar applications before to obtain the same goal?	.749	
Information Security Practices – Access Control	ISP10TA	como navego por la Web, yo permito a los navegadores aceptar cookies de los diferentes sitios Web	As I surf the Web, I allow browsers to accept cookies from Web sites (-)	.883	.718
	ISP11TA	como navego por la Web, yo permito a los navegadores la descarga de software que sea necesario.	As I surf the Web, I allow browsers to download software as necessary (-)	.883	
Information Security Practices – User Authentication	ISP01TU	cierro la sesión cuando me salgo del sistema informático.	I log off when I leave a computer system (+)	.824	.527
	ISP03TU	todas las sesiones electronicas que utilizo requieren de un unico usuario-ID y contraseña	All of my computer sessions require a unique user-id and password(+)	.824	
Information Security Practices – Security Management	ISP06TS	yo compruebo que el software de protección contra virus está activado y actualizado.	I check that virus protection software is enabled and updated(+)	.880	.708
	ISP08TS	yo examino el log del software de protección virus por actualizaciones y escaneo de dispositivos	I review virus protection software logs for updates and drive scans (+)	.880	

Table 1. Survey Items, Ractor Loadings and Reliability

		Mean	St. Dev.	1	2	3	4	5	6	7
1	SecurityAwarenessAccessControl	3.90	0.86	1						
2	SecurityAwarenessSecurityManagement	4.24	0.79	.707**	1					
3	SecurityAwarenessUserAuthentication	4.08	0.89	.678**	.677**	1				
4	Selfefficacy	3.59	0.92	.423**	.449**	.434**	1			
5	ISPUserAuthentication	3.68	1.11	.402**	.432**	.435**	.306**	1		
6	ISPSecurityManagement	3.37	1.18	.592**	.414**	.465**	.289**	.327**	1	
7	ISPAccessControl	2.81	1.06	-.068	-.108	-.032	.271**	-.106	-.089	1

** Correlation is significant at the 0.01 level; * Correlation is significant at the 0.05 level

Table 2. Means, standard deviation and correlation of Variables

RESULTS

In order to answer our first two research questions, we regressed the evaluations of information security awareness and information security practice in the three levels of access control, security management, and user authentication. Table 3 displays the beta weights and R-squared values that resulted from these three regression analyses.

	Levels of Information Security Practice		
Predictors	**SecPrac-Access Control (β)**	**SecPrac- SecurityMgmt (β)**	**SecPrac-UserAuthentication (β)**
SecurityAwarenessAccessControl	.056	.548**	.053
SecurityAwarenessSecurityManagement	-.063	-.069	.173
SecurityAwarenessUserAuthentication	.111	.130	.242**
Selfefficacy	-.296*	.018	.083
R^2	.075*	.362**	.218**

*p<.05, **p<.01

Table 3. Multiple Regression Analyses of Security Awareness and Self Efficacy predicting Information Security Practices: Access Control, Security Management, User Authentication

Several results are notable in Table 3. Although the numbers are not high, the predictors had the greatest success in predicting SecPrac-security management first as the dependent variable (.362) and then SecPrac-UserAuthentication (.218). Although the overall regression equation was statistically significant for SecPrac-AccessControl, the predictors only explained a very small amount of variance in this outcome.

Examining the signs of the beta weights for SecPrac-Security Management (related to checking for software virus protection to be enabled and updated, we found that the best predictors were SecurityAwarenessAccesssControl, related to users' knowledge about security threats (.55, p<.01). We expected to have a consistent relationship between each of the types of security awareness and security practices. However, it seems that only some key issues about security awareness are well known within this population, specifically those related to access control. However, many of our participants knew very little about security management such as the need for frequent updates of virus protection software and reference to virus protection policies. The results about self-efficacy showed that self-efficacy only explained a very small amount of variance in this outcome, with less than 1* of R square in each case.

Comparisons of Group Means by IT Career and Gender

In order to answer our RQ3, we conducted comparisons between group means and analysis of variance (ANOVA). Table 4 contains a list of the dimensions of information security awareness, self-efficacy and information security practices as defined in Table 1. We conducted a comparison between males and females and a second comparison between people in IT careers who have more knowledge of information security and people in non-IT careers. Results showed that males reported information security practices of security management greater than females (mean of 3.57 for males vs. 2.93 for females) with a significant difference of p<.01.

As expected, people in IT careers showed higher information security awareness than people in non-IT careers. Comparisons between people in IT careers and people in non-IT careers showed two significant differences: First, that people in IT careers have more security awareness about security management and user authentication. Likewise, they reported higher means in security practice in security management.

Variable Name	IT Career	Non IT Career	t	Male	Female	T
SecurityAwarenessAccessControl	4.24	3.64	5.81	3.96	3.77	1.58
SecurityAwarenessSecurityManagement	4.41	4.10	3.09*	4.27	4.17	.90
SecurityAwarenessUserAuthentication	4.36	3.87	4.37*	4.13	4.00	1.03
Selfefficacy	3.80	3.44	3.16	3.63	3.51	.98
ISPAccessControl	2.73	2.89	-1.21	2.70	3.07	-2.59
ISPUserAuthentication	3.94	3.50	3.14	3.64	3.80	-1.05
ISPSecurityManagement	3.90	2.94	6.83*	3.57	2.93	4.02*

*p<.05, **p<.01

Table 4. Group mean differences on evaluation of IT career and gender

Finally, we ran an analysis of variance (ANOVA) by degree of education, presented in Table 5. In general, we found that people with more education reported more awareness and practice of information security. There is a significant result about Information Security Practice security management that indicates that people with more education are more careful with virus protection software update and use.

	HS N=100	Bachellor N=116	GradCert N=22	Master N=14	ANOVA F
SecurityAwarenessAccessControl	3.87	3.89	3.98	4.33	1.37
SecurityAwarenessSecurityManagement	4.18	4.22	4.48	4.49	1.13
SecurityAwarenessUserAuthentication	3.96	4.13	4.16	4.45	1.83
Selfefficacy	3.60	3.62	3.40	3.62	.57
ISPAccessControl	2.68	2.84	3.09	3.21	1.43
ISPUserAuthentication	3.66	3.59	4.23	3.79	1.68
ISPSecurityManagement	3.20	3.52	3.00	4.00	2.59*

*p<.05, **p<.01

Table 5. ANOVA by Education

CONCLUSION

Our study is one of the first quantitative studies conducted with Latin American participants, in this case Bolivian Internet users. More research about information security practices needs to be conducted in Latin America and this study is an initial contribution.

In terms of the scales used in this study, this study has attempted to further validate the information security awareness and practice scales used previously by Ryan (2006). The scales used in this study can be replicated in the future either in English or Spanish. This study makes a contribution because of its innovative use of the scale and because it was done within the context of Latin American computer users. Having this kind of scales for organizational use can help in security auditing practices to understand the current status of security awareness and practices of Internet users.

In general, Internet users in Latin American are aware of common security issues such as the need to use antivirus protection. However, there is little knowledge about security policies since many organizations do not follow formal security management practices. Our study showed that people in IT careers have more awareness about security management and user authentication. Likewise, they reported higher means in security practice in security management probably because of their technical knowledge. However, security awareness and practice it is not a task of only IT people. They are the ones in charge of the technical settings but security awareness and management practices should be important to all users in general. Training and other information sharing practices should be promoted in order to increase security awareness and practices of all Internet users.

ACKNOWLEDGMENTS

We thank all the students of the class SIS303-2/2009 of the Bolivian Catholic University who helped us in the data collection.

REFERENCES

1. Agarwal, R., Sambamurthy, V., & Stair, R. (2000). The Evolving Relationship between General and Specific Computer Self-Efficacy: An Empirical Investigation. *Information Systems Research*, 11(4), 418-430.
2. Aiken, M. S., & Hage, J. (1968). Organizational interdependence and intraorganizational structure. *American Sociological Review, 33*, 912-930.
3. Arief, B. and D. Besnard (2005). Technical and Human Issues in Computer-Based Systems Security. Centre for Software Reliability, School of Computing Science, University of Newcastle upon Tyne. Retrieved November 28, 2007 from, http://www.dirc.org.uk/publications/techreports/papers/5.pdf
4. Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review,* 84, 191-215.
5. Bandura, A. (1997). *Self-efficacy: The exercise of control.* New York: W.H. Freeman and Company.
6. Bandura, A. (2002). Social Cognitive Theory in Cultural Context. *Applied Psychology: An International Review*, 51(2), 269-290.
7. Barker, J. (1993). Tightening the iron cage: Concertive control in self-managing teams. *Administrative Science Quarterly, 38*(3), 408-437.
8. Berghel, H. (2007). Better-Than-Nothing Security Practices. Communications of the ACM, 50(8), 15-18.
9. Boss, R. S. (2007). Control, Perceived Risk And Information Security Precautions: External and Internal Motivations for Security Behavior. University of Pittsburgh.
10. Burrel, G. (1998). Modernism, post modernism and organizational analysis, in McKinlay A and Starkey K (Eds) Foucault. *Management and Organization Theory: from Panopticon to Technologies of Self*, 14-28.

11. Cardinal, L. B. (2001). Technological innovation in the pharmaceutical industry: The use of organizational control in managing research and development. *Organization Science, 12*(1), 19-36.
12. Chae, B., & Poole, M. S. (2005). Mandates and technology acceptance: A tale of two enterprise technologies. *Journal of Strategic Information Systems, 14*(2), 147-166.
13. Chen, C.C., R S Shaw, and S.C. Yang. (2006). Mitigating Information Security Risks By Increasing User Security Awareness: A Case Study Of An Information Security Awareness System. Information Technology, Learning, and Performance Journal, 24(1), 1-14.
14. Clegg, S. (1994). Power relations and the constitution of the resistant subject in Jermier JM, Knights D and Nord WR. Routledge, London.
15. Collinson, D. (1993). Strategies of resistance: Power, knowledge and subjectivity in the workplace, in Jermier JM, Knights D and Nord WR. Routledge, London.
16. Compeau, D. R. and C. A. Higgins (1995). "Application of social cognitive theory to training for computer skills." Information Systems Research 6(2): 118.
17. Compeau, D. R. and C. A. Higgins (1995). "Computer self-efficacy: Development of a measure and initial test." *MIS Quarterly 19*(2): 189.
18. Daft, R. L., & Macintosh, N. B. (1981). A Tentative Exploration into the Amount and Equivocality of Information-Processing in Organizational Work Units. *Administrative Science Quarterly, 26*(2), 207-224.
19. Daudi, P. (1986). *Power in the Organisation*. Oxford.
20. Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of information Technology. *MIS Quarterly, 13*(3), 319-340.
21. Dewar, R., & Werbel, J. (1979). Universalistic and Contingency Predictions of Employee Satisfaction and Conflict. *Administrative Science Quarterly, 24*(3), 426-448.
22. Dhillon, G. and Backhouse, J. (2001) "Current Direction in IS Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal*, 11, 127-153.
23. Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125-128.
24. Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies *. Journal of the Association for Information Systems, 8(7), 386.
25. Eisenhardt, K. M. (1985). Control: Organizational and economic approaches. *Management Science, 31*(2), 134-149.
26. Goodhue, D.L. and Straub, D.W. 1991. Security concerns of system users: A study of perceptions of the adequacy of security, *Information & Management* 20, 13-27.
27. Hall, R. H. (1968). Professionalization and bureaucratization. *American Sociological Review, 33*, 92-104.
28. Hartwick, J., & Barki, H. (1994). Explaining the Role of User Participation in Information System Use. *Management Science, 40*(4), 440-465.
29. Havelka, D. (2003). "Predicting software self efficacy among business students: A preliminary assessment." *Journal of Information Systems Education* 14(2): 145.

30. Hayashi, A., C. Chen, et al. (2004). "The Role of Social Presence and Moderating Role of Computer Self Efficacy in Predicting the Continuance Usage of E-Learning Systems." *Journal of Information Systems Education* 15(2): 139.
31. Hu, Q., Hart, P., and Cooke, D. (2006) "The Role of External Influences on Organizational Information Security Practices: An Institutional Perspective," Proceedings of the 39th Hawaii International Conference on Systems Science (HICSS 39), January 4-7, Hawaii, USA. CD-ROM, IEEE Computer Society.
32. Jermier, J. M., Knights, D., & Nord, W. R. (1994). *Resistance and Power in Organisations*. Routledge, London.
33. Jermier, J., & Clegg, S. (1994). Critical issues in organization science: A dialogue. *Organization Science, 5*(1), 1-13.
34. John, L. (2003). Improving user security behavior. *Computer & Security*, 22(8).
35. Kirsch, L. J. (1996). The Management of Complex Tasks in Organizations: Controlling the Systems Development Process. *Organization Science, 7*(1), 1-21.
36. LaRose, R., & Eastin, M. S. (2004). A Social Cognitive Theory of Internet Uses and Gratifications: Toward a New Model of Media Attendance. *Journal of Broadcasting & Electronic Media 48*(3):
37. Leach, J. (2003). Improving user security behavior. *Computer & Security, 22*(8), 685-692.
38. Lee, C.-C., H. K. Cheng, et al. (2007). "An empirical study of mobile commerce in insurance industry: Task-technology fit and individual differences." *Decision Support Systems* 43(1): 95.
39. Lindholm, l. (2006). Security Awareness. Retrieved, 2008, from the World Wide Web: http://csrc.nist.gov/organizations/fissea/2006-conference/Lindholm-FISSEA2006.pdf
40. Ma, Q., & Pearson, J. M. (2005). ISO 17799: "Best Practices" in inforamtion security management? *Communications of the Association of Information Systems, 15*, 577-591.
41. Marakas, G. M., M. Y. Yi, et al. (1998). "The multilevel and multifaceted character of computer self-efficacy: Toward clarification of the construct and an integrative framework for research." *Information Systems Research* 9(2): 126.
42. Marakas, G. M., R. D. Johnson, et al. (2007). "The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time." *Journal of the Association for Information Systems* 8(1): 15.
43. Mills, E. (2009). *Study: Cybercrime cost firms $1 trillion globally*. Retrieved, from the World Wide Web: http://news.cnet.com/8301-1009_3-10152246-83.html
44. Ouchi, W. G. (1977). Relationship between Organizational-Structure and Organizational-Control. *Administrative Science Quarterly, 22*(1), 95-113.
45. Pfeffer, J., & Fong, C. T. (2005). Building Organization Theory from First Principles: The Self-Enhancement Motive and Understanding Power and Influence. *Organization Science, 16*(4), 372-388.
46. Reed, K., D. H. Doty, et al. (2005). "The Impact of Aging on Self-efficacy and Computer Skill Acquisition." *Journal of Managerial Issues* 17(2): 212.
47. Robey, D. (1979). User Attitudes and Management Information System Use. *Academy of Management Journal, 22*(3), 527-538.

48. Ryan, James Emory (2006) A comparison of information security trends between formal and informal environments. Ph.D. dissertation, Auburn University, United States -- Alabama. Retrieved October 22, 2007, from ProQuest Digital Dissertations database. (Publication No. AAT 3225287).
49. Seeck, H., & Kantola, A. (2009). Organizational control: Restrictive or productive? *Management & Organization, 15*(2), 241-257.
50. Sheng, Y. P., J. M. Pearson, et al. (2003). "Organizational culture and employees' computer self-efficacy: An emperical study." *Information Resources Management Journal* 16(3): 42.
51. Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31.
52. Smith, S. M. (2005). "The Digital Divide: Gender and Racial Differences In Information Technology Education." *Information Technology, Learning, and Performance Journal* 23(1): 13.
53. Stanton, J. M., & Stam, K. R. (2006). The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets - Without Compromising Employee Privacy or Trust. Medford, NJ: Information Today, Inc.
54. Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of End User Security Behaviors. *IEEE International Conference on Systems, Man and Cybernetics,* 2501-2506.
55. Straub, D. W. and Welke, R. J. 1998. Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly,* 22, 4, 441-469.
56. Suminski, R. R., & Petosa, R. (2006). Web-Assisted Instruction for Changing Social Cognitive Variables Related to Physical Activity. *Journal of American College Health Journal of American College Health J1 - Journal of American College Health, 54*(4), 219-225.
57. Taneja, A. (2006). Determinants of adverse usage of Information Systems Assets: A study of antecendents of is exploit in organizations.
58. Thatcher, J. B. and P. L. Perrewe (2002). "An empirical examination of individual traits as antecendents to computer anxiety and computer self-efficacy." MIS Quarterly 26(4): 381.
59. Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal Computing: Toward a Conceptual Model of Utilization. *MIS Quarterly, 15*(1), 125-143.
60. Timms, S., Potter, C., & Beard, A. (2004). *Information security breaches survey 2004*. Retrieved, from the World Wide Web: http://www.infosec.co.uk/files/DTI_Survey_Report.pdf
61. Torkzadeh, G., J. C.-J. Chang, et al. (2006). "A contingency model of computer and Internet self-efficacy." Information & Management 43(4): 541.
62. Vara, V. (2007). Ten Things Your IT Department Won't Tell You. *Wall Street Journal*, pp. R1.
63. UniversiaKnowledge@Wharton. (2008). *For Latin American companies, data theft poses a serious threat*. Retrieved, from the World Wide Web: www.wharton.universia.net/index.cfm?fa=viewfeature&id=1560&language=english
64. Wilson, T. (2006). *How much does a Hack cost?* Retrieved from the World Wide Web: http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=208803989