https://doi.org/10.48009/2_iis_2009_299-308

PERCEPTIVE PROFILES OF STUDENTS COMPUTER SECURITY & SAFETY COMPETENCIES: IMPLICATION FOR BUSINESS CURRICULUM

Dr. Ewuuk Lomo-David, North Carolina A&T State University, lomoe@ncat.edu

ABSTRACT

The frequency with which intruders successfully breach and create havoc on computer systems and networks seems to indicate that information technology (IT) personnel and other employees whose duties are to protect these systems are either ill-prepared for their jobs, unfamiliar with information technology security measures (ITSM) or just not savvy enough for the industry. This issue seems to suggest that employers should seek to recruit student applicants (prospective employees) whose profiles relate to familiarity with ITSM. The profiles (gender, academic classification, academic majors, and experience with computers) have significant relationships with familiarity with ITSM (passwords, scan of computer systems and email attachments, functions of anti-virus software, placements of passwords on email attachments, functions of biometric authentication, firewalls, intrusion detection systems, and multifaceted authentication systems). Multiple regression analysis of data from a survey of 867 Nigerian university students revealed that engineering and business majors; and students with very good computer experience tend to be familiar with all ITSM except sophisticated passwords and functions of multifaceted authentication systems. Students who possess documentable familiarity with ITSM may make better information security-savvy employees that can engender much needed trust in the IT industry and profession.

Keywords: Information technology security measures (ITSM), Nigerian university students, NIDTA, password protection, intrusion detection systems, authentication systems.

INTRODUCTION

The rate at which intruders and hackers successfully breach computer systems with impunity across the corporate world and educational institutions seem to indicate that some IT personnel and other employees tasked to protect systems are unable to offer appropriate protection, may be unfamiliar with ITSM and may also lack requisite training. The unfamiliarity and attendant digital insecurity are exacerbated by human-driven rogue computer malware and illicit intrusions into computer systems Reagan [23]. Each time there is a breach companies lose money because of a variety of complex issues. Some of those issues include the more than $14 million that companies lose in court costs and loss of productivity, explained Hall [12]. Each successful system breach and attendant financial, information, and manpower loss set of a ripple effect that negatively affects the breached company and its immediate and extended customer base. Teer [27] found that undergraduate students share their passwords and have relatively insecure computers and computing practices, thus calling into question their extended interest in the value of what is learned in college.

Computer security breaches may be intentional and generated internally, Leach [18] or from external sources. The internal threat, usually by aggrieved employees, may be addressed by scheduled IT personnel/other employee training on appropriate security practices and fair treatment of employees. External threats can be addressed by harnessing all internal security measures and intranet monitoring. Since students are the next group of prospective employees, it is necessary for employers to understand students' level of familiarity with secure computing practices in order to provide appropriate in-house training. Students computing practices add less credence to their computer security and safety stance. The literature indicates that 49% of business students are not well-trained to avoid risky computing behaviors expressed Aytes and Connolly [2]. When students are found to be deficient in the content of their learning, teachers tend to be rightfully responsible. The foregoing statement makes it necessary to determine how savvy, relative to ITSM, current university students will be at graduation. The results of this study may call for adjustments to college curricula that prepare students from all disciplines for a digitally secure world. The remainder of this paper will discuss literature review, purpose of the study, research hypotheses, methodology, data analysis, results, discussion and conclusion.

LITERATURE REVIEW

Management and security of computers and digital information have been of major concern to all facets of the global economy since the advent of computers, digital networks and electronic data storage and transmission. Mass media reports of continual compromises of computer systems and loss of digital proprietary information have generated intense interest in studies of information systems vulnerabilities across disciplines. A casual perusal of most university catalogs shows course offerings in information security. Also, a Google search of journals serving information security research interests shows how widespread the topic is in academia and in practice. The current review will explore academics' and practitioners' literature from three perspectives: 1) reasons for successful computer security breaches, 2) documented computer security breaches, and 3) countering threat of intrusion, disablement and offering solutions. Literature search revealed a paucity of information on student familiarity with ITSM.

Reasons for Successful Security Breaches

Researchers continue to examine computer security breaches and attempt to explain reasons for its pervasiveness. Between 1995 and 2000, vulnerabilities and attacks rose 637.43% and increased to 3,508 by 2005 thus exposing several organizations to expensive security breaches. An FBI report by Zang & Li [31] adds that there is a 90% chance of computer breaches in today's companies that will result in a financial loss of 80%. The report stresses that a possible 44% of these companies will lose in excess of $4 million.

Lack of relevant security skills for the entire work force has been blamed for security problems. In searching for relevant skills, as ranked for the Chief Information Security Office (CISO) by research and job listing, Whitten [30] reports that the CISO critical skills requirements are "management skills, information systems security education, a broad array of soft skills, disaster recovery planning and security breach investigations." Business strategy, which should involve security, did not appear in the most included job duties even though the literature and executives gave it prominence in ranking. Organizations invest money in security training of employees to forestall security issues Gordon [11] but the threat continues to be real, disenchanting and evolving. Because the threat is evolving and its source is generally ubiquitous and ambiguous, it continues to be difficult to anticipate and impede its nefarious progress prior to serious breach.

Security of information objectives Ma [19] which comprises integrity, confidentiality, accountability and availability should be treated as a management issue rather than a technical one. If organizations embrace information security management (ISM) properly, breaches and systems crashes may be avoided. Both medium and small sized companies consider system access control by management to be important security practice. To ensure that security consciousness permeates the entire organization, CISO should be involved in security training and education that merges security management and business process, expressed Kubilus [16].

Mullins [20] posts that the low information technology budget allocation by management compared to other divisions contributes to the ill preparedness of IT to prevent intrusions. A survey of 500 risk and IT managers indicates that there is not enough action to assess risks related to cyber activity. Emrich indicated that organizations have not developed a holistic view of security and regulatory compliance and have not implemented a single business process control that includes identity and access management (I&AM) that taps into user identity [7].

Modern mobile phones and digital devices according to Dornan have increasingly greater processing power, are primarily based on Palm operating systems and can handle more sophisticated software [6]. These greater processing powers coupled with the ability to connect through Bluetooth devices to the internet provide the uncomfortable recipe for virus download, replication and distribution to networks. As companies implement newer technologies, more questions arise regarding the security of these actions Kirk [15]. A case in point is the looming implementation of IP networks convergence by 62% of companies while only 63% of these same companies expect this action to result in a higher level of security. One would expect a higher percentage of companies to implement IP convergence because of economies of scale and cost reduction benefits. Several companies react to threats and breaches only as an afterthought said Vijayan [28]. In some cases, by the time the latent reaction occurs, the damage is already done and costs millions of dollars to correct the problem, rebuild goodwill and finally publish the incident, as required by law stated White [29].

Documented Computer Security Breaches

Data theft and malicious break-ins are on the rise Caruso [4]. In 1977, security breaches occurred on almost 77 million records in U.S.A., according to the San Diego Identity Theft resource Center. To combat these problems companies and governments are trying different data protection and control methods such as "1) using new protocols and frameworks for collecting data, using and governing identity data in such a way that companies can eventually improve their public relations and dowse legal problems arising from customer data tampering, 2) shifting the burden of carrying customer data to the customer by deploying CloudTripper Project, 3) Identity Governance Framework which will enable organizational compliance with regulations such as the Sarbanes-Oxley Act and the Health Insurance Portability and Accounting Act. Identity Governance Framework, widely accepted by major software companies share and audit sensitive personal information, 4) the concept of legally recognizable "Limited Liability Persona (L.L.P)" creation in which individuals will register and have their own L.L.P. with mailing address, tax identity and other information. The benefit is that L.L.P. will be treated like property and the owner of this property will only be penalized for a limited amount of money loss in case a theft of identity occurs.

Executive officers are frustrated that some companies do not even know when they have had a security breach stated Emrich [7]. To add to that, Chief Executive Officers (CEOs) view computer security as being encumbered by many domestic and global regulations while Chief Financial Officers (CFOs) view it as a cost problem that must be invested in technologically. These divergent views create distrust between these executives. To ensure that security is controlled properly, a succinct plan for "identify and access management" system that "provides an absolute audit and log of what every user in your organization had access to, when they gained access and what they did" will be required. Reagan [23] reports that computer hackers used a malware to breach computers at Hannasford Supermarkets in Massachusetts by successfully capturing credit card numbers of customers and forwarding this malicious malware to 300 computer servers that stored customers' information. It was a novel approach to cyber crime whereby customer information stored in a central location was compromised by the malware retrieving and distributing identification information on cards' magnetic stripes at the point of sale to hackers. Central storage of customer information is against the Payment Card Industry (PCI) data protection standard. Fallon of Worcester Massachusetts, a health care provider patient database was compromised when a laptop with 30,000 unencrypted personal diagnostic information was stolen Hollmer [13].

Network breaches are not only orchestrated by disgruntled employees but also surprisingly by reputable competitor companies that hope to pilfer valuable information for competitive advantage. In early 2008, a multimillion dollar settlement was reached by two companies in Idaho in which one of the companies hacked into the other company's database to steal valuable information, Shifrin [25]. The terms of the settlement precluded public identification of litigants in order to forestall public relations damage. The probable protection of identity of security perpetrator firms from public knowledge hardly sounds a warning to would be perpetrators.

The Plug and Play feature of personal computers' operating systems such as Windows 2000 at Caterpillar, General Electric, and UPS were infected by a virus named Zotub that created a denial of service and left users askance Claburn [5]. A litany of companies such as CNN, Sun Microsystems, Bank of America, Dole Foods and more have been affected by viral attacks. To combat future attacks many companies aim at enhancing application security, access control management, secure remote access and adhere to the Sarbanes-Oxley Act, and for residents of California, also comply with the California law that mandates breaches disclosure. In August 2007, Monster.com's 1.6 million jobseekers' database was compromised, Bergstein [3]. An innovative form of malware, sent to Tucson newspapers on November 3, 2007, was programmed as an advertisement that clients clicked on and got redirected to a site with fake virus-scanning software, Gillum [9]. In 2003, security incidents reports were up by 137,529, as per CERT Annual Report [14]. In January 2008, OmniAmerica of Fort Worth, Texas had customer personal information stolen from its computers Shlacter [26]. Vijayan [28] reported the following incidents regarding security breaches: T. Rowe Price disclosed the security breach in which 35,000 members' personal information was compromised. T.D. Ameritrade Holding Corporation's database of 6.2 million customer's personal information was stolen. Fidelity National Information Services Inc. compromised 8.2 million customers' data when a senior manager sold the company data to brokers. Her Majesty's (HM) Revenue and Customs, in November 2007, lost unencrypted disk with the personal information of 25 million tax payers in U.K. Gartner Inc. suggests that it will cost the British

government $500 million to rectify the situation. TJX companies of Framingham, MA disclosed that 45.6 million customers' cards were compromised. The intrusion continued for more than 18 months before discovery – a classic example of reacting to a threat as an afterthought. TJX suggest that it will cost $250 million to service the problem.

Countering Threat of Intrusion, System Disablement and Offering Solutions

Layland [17] posits that the increasing incidents of new successful threats on networks have prompted several companies to investigate ways to counter these problems. These new threats are no more bombarded only on the traditional network layer but transported through the application layer. Furthermore, network vulnerability is exacerbated by the fact that signatures created to capture the known viruses, worms, malware, and root kits do not have the capacity to recognize the zero-day threats which are new worms that do not have signatures yet created to combat their spread. To add to the problem, the new viruses are embedded in the application payload instead of in the packet header and then transported over a multiplicity of packets. To ensure some semblance of avid security of payload content, several measures such as "network access control", zero-day detection, and anomaly detection and behavioral modeling "web application firewalls" such as creation of "white list", "monitoring actions", "tampering" and "signatures" have to be implemented.

It is necessary to proactively deploy vulnerability management software that contains tools that can detect intruder-exploitable potentially weak software system. The market value for these tools reached $200 million in 2007 and is particularly attractive because they can check developer program codes for weaknesses and react to potential communication network weaknesses while recording scans from intruders, White [29].

Since digital information is pervasive in today's corporate environment and our continued existence depends on its being kept secure, we have to implement information protection and control (IPC) strategy. This implementation will ensure that data in transit, at rest and in use are secure, encrypted, and sensitively blocked from unauthorized access as detailed in a *Business Wire* article in an IDC Corporation's study [1]. Emrich state that the current annual corporate spending to IT division budget ratio is a mere 100:5 that barely scratches the surface of IT services needed to aggressively pursue IT interests [7]. A corporate and IT division budget ratio of 100:20, development of a holistic view of security and regulatory compliance coupled with inclusion of technology security in the business process will bolster IT division's reach and richness. Identity and access management (I&AM) should be employed to control theft and misappropriations. Also, management must provide IT the authority to maintain, contain activities, continually assess networks, be familiar with worms and viruses and assure that new network platforms meet standards set for current proactive computing indicated Dornan [6]. Employers who understand students' computing practices and ensure appropriate training Aytes [2] after hiring will reap the benefits.

Corporate training of IT security personnel is currently designed for the CIO and upper-level management instead of the lower level employees who need it. Security training would be beneficial to all levels of personnel in the organization Godwin [10], Leach [18]. Viruses that infect a computer system must first be coded by an avid programmer, introduced by a hacker who scans networks to uncover vulnerabilities and finally manipulated for a specific purpose. Based on this knowledge Zou et al. [32] suggest that stopping a virus from a successful attack and invasion is a function of differentiating between the time of "a worm's propagation" behavior which is usually based on specific codes, signals and statistical similarity; and hacker's intrusion attack which is not exactly well defined and may only target specific computers. Finally, the foregoing literature review documents the problems of systems insecurity and prepares the ground work for a succinct approach to the purpose of this study.

PURPOSE OF THIS STUDY

The purpose of this study was to determine whether the four university students' profiles (gender, major, classification and experience with computers significantly affect familiarity with ITSM. A prior study Aytes [2] did not absolve students on their computing behaviors and interest in the safety of information. In 2001, Nigerian Federal Executive Council approved a National Information Technology Development Agency (NITDA) [22] to bring information technology closer to the people by ensuring that "the entire citizenry is empowered with information technologies through the development of a critical mass of IT proficient and globally competitive manpower." The foregoing statement makes this study necessary in order to assess university students' familiarity with ITSM. Figures 1

and 2 illustrate the pre and post interaction between the four student profiles and ITSM respectively.

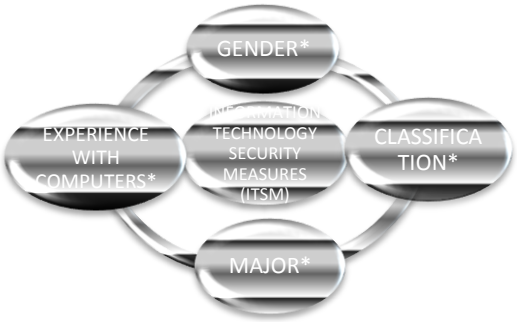

Figure 1: Graphical Representation of Possible Perceived Interaction between Student Profiles* and ITSM before Regression Analysis

Definitions: 1) Information technology security measures are safe computing attributes (Table 1). 2) Simple passwords comprise characters that can be easily guessed. 3) Sophisticated passwords comprise character combinations of more than 8 and not easily guessed. 4) Student profiles in this study are "gender, major, academic classification, and experience with computers".

RESEARCH HYPOTHESES

The ten null hypotheses tested in this study are in Table 1.

Table 1: Research Hypotheses

No.	**Activities**
	There is no significant relationship between the four student profiles: 1. Gender, 2. Classification (undergraduate-graduate), 3. Major (Arts & Science, Business, Engineering and Others), 4. Experience with computers (Expert, Very Good, Good, Poor) and the following:
$H_0$1	familiarity with simple passwords
$H_0$2	familiarity with sophisticated passwords
$H_0$3	familiarity with daily computer systems scans
$H_0$4	familiarity with scanning of email attachments
$H_0$5	familiarity with functions of anti-virus software
$H_0$6	familiarity with placement of passwords on email attachments before sending
$H_0$7	familiarity with functions of biometric authentication
$H_0$8	familiarity with functions of firewalls
$H_0$9	familiarity with functions of intrusion detection systems
$H_0$10	familiarity with functions of multifaceted authentication systems

METHODOLOGY

Literature review provided the material for the development of a Likert-type questionnaire used for this research. The first part comprised ten statements that sought to identify the level of Nigerian university students' familiarity (extremely familiar, very familiar, familiar, barely familiar, not familiar) with ITSM. The second part sought to identify respondents' profiles (gender, major, classification, and experience with computers). The questionnaire was reviewed by colleagues in a U.S. southeastern university, a Nigerian university, a healthcare institution in Wales (United Kingdom) and Nigeria Liquefied Natural Gas Company for suitability and appropriateness. A pilot test of the questionnaire on 100 students resulted in elimination of ambiguities. For a formal administration of the survey a faculty member in each participating university was identified to administer 100 questionnaires to students within the academic year. All participants and institutions were promised anonymity. A total of 1,100 students (55%) of 2,000 who were contacted returned 867 (78.8%) usable questionnaires after email reminders. Twenty of the 90 universities in Nigeria that are members of the National Universities Commission (NUC) [21], the main higher education

accrediting institution of Nigeria were randomly selected.

DATA ANALYSIS

The analysis of this study was conducted with descriptive statistics and multiple regressions. The independent variables (profiles) are gender; major (Arts & Science, Business, Engineering, Others); classification (graduate, undergraduate); Experience in computing (expert, very good, good, poor/novice). The ten dependent variables are presented in Table 2.

RESULTS

Study Profiles

Four hundred sixty four (53.5%) of the respondents were female. Most respondents were undergraduate (62.5%) and graduate (37.5%) with academic majors in Arts & Sciences (28.7%), Business (37.3%), Engineering (18.3%) and Others (15.7%). Respondents' level of experience in computing were Expert (45.8%), Very good (22.1%), Good (18.3%), Poor/Novice (13.7%).

Table 2: Regression – Showing Results Obtained From Each Hypothesis

	ITSMs (dependent variables)	Student Profiles (independent variables)	Beta β	T	Effect Size††	R^2	α= 0.05
$H_0$1	Simple passwords to protect computer data	Major(Engineering) Major(Business) Major(Others) Experience(Very Good)	.300 .263 .106 .073	7.8+ 6.6+ 2.8+ 2.0+	.94 .92 .71 .58	.095	.000 *
$H_0$2	Sophisticated passwords to protect computer data	Gender Experience(Poor)	-.069			.015	.123
$H_0$3	Daily computer system scan	Gender Major(Engineering)	.284 .141	8.8+ 3.7+	.95 .80	.127	.000*
$H_0$4	Scan of email attachments	Experience(Very Good) Experience(Poor) Experience(Good) Major(Business) Class (Undergrad/Grad)	-.303 -.189 -.177 -.140 .089	-8.7+ -5.5+ -5.2+ -3.6+ 2.8+	.95 .89 .88 .79 .70	.141	.000*
$H_0$5	Functions and usage of anti-virus software to check for viruses	Experience(Very Good) Major (Others) Experience (Good) Experience (Poor) Major (Business)	-.369 -.284 .205 -.156 -.156	- 10.9+ -7.9+ -6.2+ -4.7+ -4.2+	.97 .94 .91 .86 .83	.196	.000*
$H_0$6	Placing passwords on email attachments	Gender	.132	3.9+	.81	.026	.004*
$H_0$7	Functions of biometric authentication	Major (Others) Gender Major (Business)	.160 .138 .126	4.1+ 4.1+ 3.1+	.83 .82 .74	.051	.000*
$H_0$8	Function of firewalls as security measures	Major (Others) Gender	.135 .127	3.7+ 3.5+	.79 .78	.040	.000*
$H_0$9	Function of intrusion detection systems	Experience (Poor) Experience (Good) Gender	.100 -.113 -.092	2.8+ -3.1+ -2.7+	.70 .74 .69	.040	.000*
$H_0$10	Functions of multifaceted authentication systems	Gender	.069			.015	.115

*=sig. alpha, P<.05, +t = > 2; ††r=$\sqrt{(t^2/t^2+df)}$ used to determine effect size; β =st'dized regression coefficient

Hypotheses Tested

Regression analysis [Enter] in SPSS 15 was used in this study by regressing student profiles "independent variables" on each of the 10 dependent variables. The following rationalizations are based on results in Table 2. The primary null hypotheses (H_o) is that there is no significant relationship between the student profiles – Gender, Major (Arts & Science, Business, Engineering and Others) Classification

(undergraduate-graduate), Experience with computers (Expert, Very good, Good, Poor/novice) and familiarity with the 10 ITSMS (Table 1).

H_o1: Simple passwords. Regression analysis produced an overall significant probability value of .000 at $p < .05$. The null hypothesis is rejected. There is a significant relationship between student profiles and familiarity with simple passwords. The regression coefficients (β=Beta) for Major (Engineering) = 0.300, t=7.823; Major (Business) =.263, t=6.586; Majors (Others) =.106, t=2.812, and Experience (Very Good) =.073, t=2.034; thus showing in descending order, the effect contributed by each predictor variables to the significant relationship, Reinard [24]. The t-statistic (all greater than 2) further confer stability on the observed levels of significance because the rule of thumb is that t =>2 indicates significance. To ensure that chance is not the probable cause of the significant effect, according to Reinard, [24] the size of effect of each significant independent variable is further determined by $r = \sqrt{(t^2/t^2 + df)}$ where r = effects size, t=observed t statistic, df=degrees of freedom. Calculating effect size for Major (Engineering), $r = \sqrt{((7.823)^2/(7.823)^2 + 8))} = \sqrt{(61.199/61.199) + 8)} = \sqrt{.88434} = .94$. This is a large effect size. Other predictor variables' effect sizes are Major (Business) = 0.92, Major (Others) = .70, and Experience (Very Good) = 58. The r^2=.095 indicates 9.5% of variation in familiarity with simple passwords is attributable to student profiles.

H_o2: Sophisticated passwords: β = -.069, (p=.123, p<.05). The null hypothesis cannot be rejected. No significant relationship between student profiles and familiarity with sophisticated passwords.

H_o3: Daily computer system scan: β for Gender =.284; t=8.801, effect size = .95; and Major (Engineering) =.141, t = 3.731, effect size = .80 at (p = .000, p < .05). The null hypothesis is rejected. There is a relationship between student profiles and familiarity with use of daily computer system scan. The greatest effect of the positive relationship was contributed by Gender followed by Major (Engineering). The R^2 of .127 indicates that 12.7% of the variation in familiarity with daily computer system scan is attributed to student profiles.

H_o4: Scanning of email attachments: β for Experience (Very Good) =-.303, t = -8.684, effect size=.95; Experience (Poor) = -.189, t = -5.486, effect size = .89 at (p =.000, p < .05). The other contributors to the significant effect are Experience (Good)= .88; Major (Business)=.79; and Classification =.70. The null hypothesis is rejected because there is a significant relationship, though negative, between student profiles and familiarity with scanning of email attachments. The greatest effect of the negative relationship was contributed by Experience (Very Good). The r^2 of .141 indicates that 14.1% of the variation in familiarity with daily computer system scan is attributed to student profiles. The negative beta coefficients show an inverse relationship.

H_o5: Functions and usage of anti-virus software: β for Experience (Very good) is -.369, t = -10.937, effect size=.97; Major (Others) is -.284, t = -7.982, effect size=.94 at (p = .000, p < .05). The null hypothesis is rejected. There is therefore a relationship between student profiles and familiarity with functions of anti-virus software to check for viruses. The greatest effect of the inverse relationship was contributed by Experience (Very Good), with r^2 of .196 indicating that 19.6% of the variation in familiarity with functions and usage of anti-virus software is attributed to student profiles. Other effect sizes are in Table 2.

H_o6: Placement of passwords on email attachments: β for Gender is .132, t = 3.885, effect size=.81, (p = .004, p < .05). The null hypothesis is rejected. There is a relationship between student profiles and familiarity with placement of passwords on email attachments before sending. The r^2 of .026 indicates that 2.6% of the variation in familiarity with placement of passwords on email attachments before sending can be attributed to student profiles.

H_o7: Functions of biometric authentication: β for Major (Others) is .160, t = 4.142, effect size=.83 with (p = .000, p < .05). The null hypothesis is rejected. There is a relationship between student profiles and familiarity with functions of biometric authentication as a security measure. The r^2 of .051 indicates that 5.1% of the variation in familiarity with functions of biometric authentication is attributed to student profiles.

H_o8: Functions of firewalls: β for Major (Others) is .135, t = 3.743, effect size =.79 with (p = .000, p < .05). The null hypothesis is rejected. There is a relationship between student profiles and familiarity with functions of firewalls. The r^2 of .040 indicates that 4.0% of the variation in familiarity with functions of firewalls is attributed to student profiles.

H_o9: Functions of intrusion detection systems: β for Experience (Poor/Novice) is .100, t = 2.750, effect size=.70 with (p = .000, p < .05). The null hypothesis is rejected. There is a relationship between student profiles

and familiarity with intrusion detection systems. The r^2 of .040 indicates that 4.0% of the variation in familiarity with the functions of intrusion detection systems is attributed to student profiles.

H_o10: Functions of multifaceted authentication systems: $\beta = .069$, $p = .115$, $p < .05$. The null hypothesis cannot be rejected because student profiles are not significantly related to familiarity with functions of multifaceted authentication systems.

Note: Durbin-Watson statistic ranged from .83-1.9 for all hypotheses thus indicating a possible autocorrelation but not substantially low to raise eye-brows in the study [8].

DISCUSSION

Discussion

This paper contributes to the body of knowledge on information technology security by critically analyzing the relationship between student profiles (gender, major, academic classification, experience with computers) on the one hand and familiarity with information technology security measures (ITSM) on the other.

The results depict significant influence of student profiles on 8 of 10 ITSM (Table 2). Considering familiarity with simple passwords, Engineering and Business students and students with very good experience in computing are familiar with simple passwords.

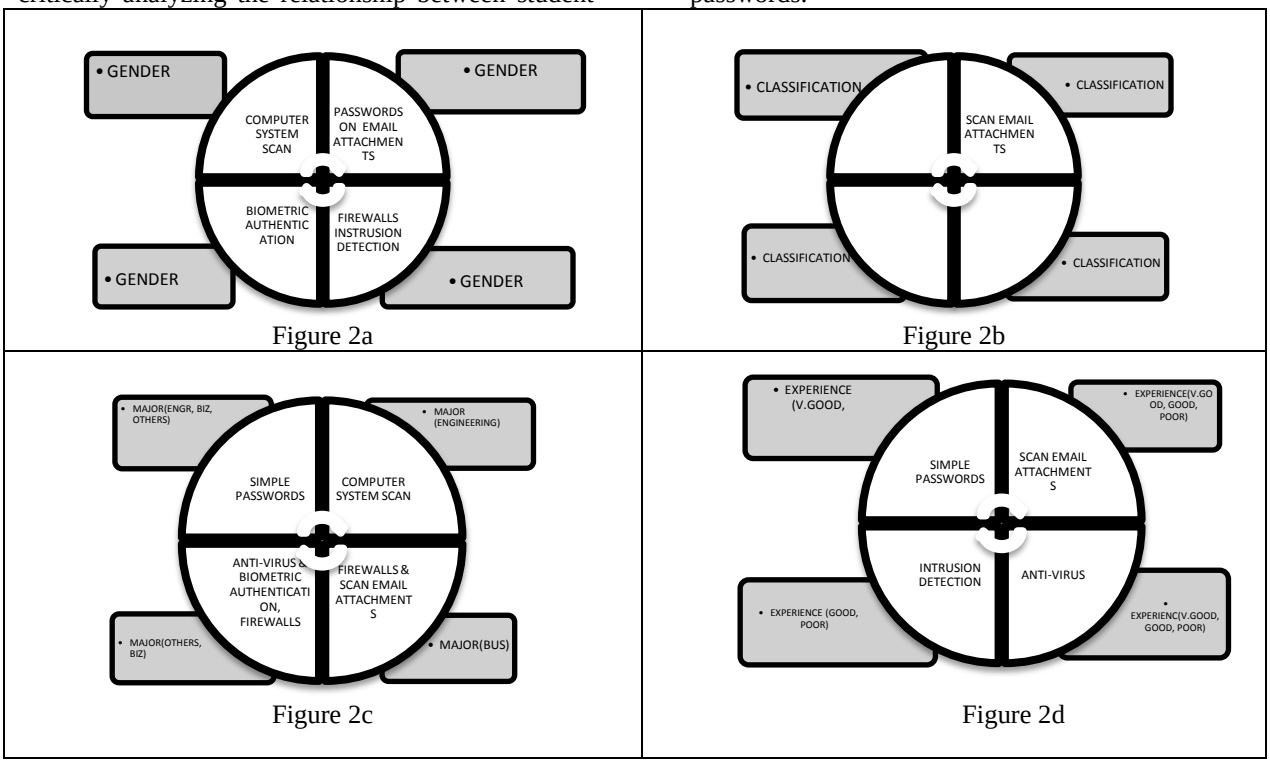

Figure 2: Graphical Representation of Post Interaction of Familiarity with ITSM and Profiles showing significant relationships

No relationship was found between student profiles and familiarity with sophisticated passwords.

Familiarity with computer systems scan is influenced by gender and engineering majors thus indicating that students in engineering are likely to be more familiar with the functions of daily computer systems scan. In today's computing environment, system scan is a necessary automated prelude to system access.

Regarding scanning of emails attachments, students with all levels of experience with computers and business majors tend to be familiar with the process. Because scanning of email attachments is today an automated process, some computer users may not be aware that email scan is an ongoing process and is a necessary prelude to daily computing. What is surprising is that respondents with poor computing experience are familiar with scanning of email attachments. This is an indication that poor experience with computers may not necessarily translate into poor familiarity with some ITSM.

Protecting computer systems can be enhanced by familiarity with anti-virus software. This familiarity tends to be expressed more by students who have all levels of experiences with computing and those studying business. It is surprising that engineering majors seemed to be unfamiliar with anti-virus software.

Gender influences familiarity with placement of passwords on email attachments before sending. All the other profiles do not influence placement of passwords on email attachments because people generally, unless required by the nature of their jobs, do not take that extra precaution of password creation and placement on file attachments before emailing. Microsoft Word and Excel provide an easy security means of placing a password on a document before saving.

Business students tend to be familiar with functions of biometric authentication. Gender also influences familiarity with functions of biometric authentication. The availability of biometric authentication in personal computing environment is a phenomenon that has not made much inroad into the business and classroom environment.

Familiarity with functions of firewalls is influenced by gender and other majors excluding Engineering, Arts & Sciences, and Business. The functions of firewalls do not become apparent until data loss or malware invasion of computer systems occur.

Also, gender and good to poor experience with computers influence functions of intrusion detection systems. There is an inverse relationship here. Finally, there is no relationship between multifaceted authentication systems and student profiles.

CONCLUSIONS

Since the study suggests that Arts & Sciences students do not seem to be familiar with simple passwords, efforts should be made by teachers in those disciplines to emphasize file and systems protection in their teaching. Familiarity with sophisticated passwords is not the forte of students and should raise eyebrows among teachers and in the industry. This result is in consonance with the findings of Aytes and Connolly [2], Teer [27] that students computing behaviors are security averse or not very safe. Student apathy to data safety measures is enigmatic because of ongoing public flurry of reports on unsafe computing and loss of confidence in safety of proprietary information. Very succinct efforts should be made to teach students how to use sophisticated passwords in their daily affairs with computers.

Even though student profiles and familiarity with daily computer systems scan has a general level of relationship, only gender and students in engineering are identified as contributing to this relationship. This result shows that students in other disciplines and levels of experience may not be aware of the existence of daily computer system scan for malicious agents. Even though all the predictor variables contributed a variation of 12.5%, the two strongest student profiles, gender and major (engineering) have high effect sizes of .95 and .80 respectively.

Almost all predictor variables contribute to a variation of 14.1% with a general level of relationship with scanning of email attachments. Students do want to avoid viruses and therefore are familiar with scanning of emails. This finding does not support Aytes & Connolly [27]. The irony here is that email scanning, on some computing systems, is an automatic process that both neophytes and adept users may not even notice when in process.

The understanding of multifaceted authentication systems will be beneficial for students who probably will become managers where they may be employed after graduation. Employers can also use these ITSMs as guides for training new employees to enhance security readiness.

While the result from this work call for further research to analyze familiarity with and usage of ITSM, it should also call for a critical look at the current academic curricula and determine the points at which infusion of required digital safety and security theory and practice should begin. The replication of this study in the United States and other countries would add to the discourse on computer security. A comparative analysis of opinions of practitioners and academics could provide an even more interesting set of results.

REFERENCES

1. *Business Wire*. "Protecting what's Yours: Data Loss Prevention (DLP) Emerges as a Critical Component to Organization's Overall Information Protection and Control (IPC) Strategy." http://www.idc.com. (March 20, 2008). [Accessed 4/15/08].
2. Aytes K. & Connolly T. (2004). "Computer security and risky computing practices: A rational choice perspective," *Journal of*

Organization and End User Computing 16(3), 22-40.
3. Bergstein, Brian. "Monster security breach teaches lessons," *Technology & Science*, August 31, 2007. www.msnbc.msn.com/id/20534586, [Accessed 4/15/08].
4. Caruso, D. "Securing very Important Data: Your Own," *The New York Times*, (Late Edition, East), October 7, 2007, 34.
5. Claburn, T. with Garvin M.J. "The Threats Get Nastier," *InformationWeek,*" August 29, 2005, 34-44. http://technews.acm.org/archives.cfm?fo=2005-09-sep/sep-02-2005.html#item18.
6. Dornan, A. "Airborne virus", *Network Magazine*, (15:12), December 2000, 46.
7. Emrich, A. B. (2005). "Information Security Poses Increasing Problems," *Grand Rapids Business Journal*, (23:11), March 14, 2005, 10.
8. Durbin, J., and Watson, G.S., (1950). "Testing for Serial Correlation in Least Squares Regression 1" *Biometrika*, 37, 409-428.
9. Gillum, J. (2007). "Maliciously coded online ad caused Star's Web site problem," *Arizona Daily Star. www.dailystar.com,* November 3, 2007, [Accessed 4/15/08].
10. Godwin, B. (2005) "Investment in security training on the wrong track, say Senior Staff," *Computer Weekly*, 29, November 2005, 58.
11. Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Richardson, R. "2004 CSI/FBI Computer Crime and Security survey," *CSI Publications*, June 11, 2004. www.crime-research.org/news. [Accessed 9/12/08].
12. Hall, M. (2005) "Price of Security Breaches," *Computer World* (39:46), November 14, 2005, 8.
13. Hollmer, Mark. (2008) "Security breach compromise Fallon patient data," *Boston Business Journal*, January 24, 2008.
14. http://www.cert.org. [Accessed 8/16/2008].
15. Kirk, J. (2005). "Survey: Execs see security concerns over IP convergence," *Computerworld*, http://computerworld.com/networkingtopics/networking/ story/ (), 10801, 106057.html November 5, issue. [Accessed 8/16/08].
16. Kubilus, N. "IT and Security: Converging Roles," *Computer World*, November 22, 2004, 36-43.
17. Layland, R. (2006). "Application Security: Countering the Professional," *Business Communication Review 36*(9), 34-39.
18. Leach, J. (2003). "Improving user security behavior," *Computers and Security*, 22(8), 685-692.
19. Ma, Q., (2004). "A study on information security objectives and practices," *An unpublished doctoral dissertation*, Southern Illinois University, Carbondale.
20. Mullins, R. & Hamm, A. F., (2002). "Threat of cyber terror ignored," *Silicon Valley/San Jose Business Journal*, 20(5), 3.
21. National Universities Commission, Available from: http://www.nuc.edu.ng/pages/universities.asp [Accessed 4/15/07].
22. Nigerian National Information Technology Development Agency, Available from: http://www.nitda.gov.ng [Accessed 3/12/07].
23. Reagan, T. (2008). "Hannasford's breach is a warning for your PC," *The Christian Science Monitor*, Boston, MA. April 2008, 15.
24. Reinard, J. C. (2007). *Introduction to Communication Research* 4th Ed., McGraw-Hill, Boston, MA, 2007, 509-512.
25. Shifrin, S. (2008) "You have been hacked," *The Idaho Business Review*, Boise, June 30, 2008.
26. Shlacter, B. (2008). "Gang of hackers hits Texas bank," McClatchy Newspapers, January 25, 2008. www.sacbee.com/103/v-print/story/660690.html. [Accessed 6/6/08]
27. Teer, F. P., Kruck, S.E., and Kruck, G.P. (2007). "Empirical Study of Student's Computer Security - Practices/Perceptions" *Journal of Computer Information Systems* 47(3), 105-110.
28. Vijayan, J. (2008). "Hacks, Heists and Breaches: The Security Hall of Shame," *Computerworld* 42(9), 38.
29. White, B. (2008). "Business Solutions; Where the Holes Are: New tools help companies identify the real security risks in their computer systems before the hacker," *The Wall Street Journal*, (Eastern edition), New York, N.Y. June 9, 2008.
30. Whitten, D. (2008). "The Chief Information Security Office: Analysis of the skills required for success," *Journal of Computer Information Systems* 48(3), 2008, 15-19.
31. Zang, C., and Li, S. (2006). "Security Information Sharing and Internet-Based supply Chain Management Systems," *Journal of Computer Information Systems* 46(4), 2006, 18-24.
32. Zou, C.C., Gong, W., Towsley, D. and Gao, L. (2005). "The Monitoring and Early Detection of Internet Worms," *IEEE/ACM Transactions on Networking* (13:5), 961-974.