https://doi.org/10.48009/1_iis_2013_278-285

STUDENT PERCEPTIONS OF BUSINESS COMPLIANCE WITH PAYMENT CARD INDUSTRY SECURITY REQUIREMENTS: A CONSTRUCTIVIST APPROACH

Barbara Jo White, Western Carolina University, whiteb@email.wcu.edu
Lorrie Willey, Western Carolina University, lwilley@email.wcu.edu
Ronnie Stillwell, Western Carolina University, stillwel@email.wcu.edu

ABSTRACT

Introducing students to industry standards supports one of the basic aspects of constructivism in that using standards in the classroom provides real world and authentic information from which students can develop, or construct, knowledge. Since students come to the classroom with some familiarity with data security, use of the PCI DSS requirements in classroom activities provides the means by which students can explore new information that both challenges and enhances their preexisting concepts of security. The challenges students face in ranking the difficulty of PCI DSS compliance for business represents a challenge that is also experienced by business owners. Before information systems students are able to help businesses manage risks associated with accepting credit cards, it is important to first educate them about the PCI DSS requirements. Using the constructivist approach, the first step is to understand where students are before creating activities to take them further. This paper presents a study that examines students' perceptions of the PCI DSS requirements. Specifically, the data illustrates the desire to know what students thought about the difficulties business face when complying with the 12 requirements in the PCI DSS in order to allow students to explore the complexities of data security.

Keywords: Industry Standards, Constructivism, Payment Card Industry and Data Security

INTRODUCTION

Introducing students to standards in industry, such as those in place for the retail card payment industry, is a beneficial way to let them learn about the real world by providing a glimpse of future challenges and expectations in a safe environment where mistakes are not costly. The use of industry standards in the classroom also supports the epistemology of constructivism, which provides that students build new knowledge on preexisting knowledge, and are encouraged to do so when faced with real world problems, such as data breaches. The majority of data breaches (96%) occurred in firms that were not compliant with Payment Card Industry Data Security Standard (PCI DSS) requirements and the majority of these incidents occurred in Level 4 firms with fewer than 20,000 transactions a year and with fewer than 1000 employees [32]

As educators, it is necessary to understand what knowledge students bring to the classroom in order to develop activities that will assist them in building on that knowledge so that they can contribute positively to information security measures in their future workplaces. For students in the in the core management information systems class, the Payment Card Industry Data Security Standard (PCI DSS) is an excellent choice for the classroom. These college-level students already have ideas and experiences with credit cards and with data security so most of the concepts are familiar to them. Census statistics show that industries often associated with credit card payments such as the retail trade industry, accommodation and food service, and health care are industries that employ the largest percent of workers [25]. In addition, over 99% of employing firms are considered small businesses and it is in these small businesses where it's valuable to have students working who are more knowledgeable about information security, particularly in the area where customer cardholder data is concerned [25].

Using a constructivist approach to the study of data security, the initial step is to help students, and educators, identify what the students already know about data security and then using that knowledge as the foundation for further study. Ultimately, it is hoped that students graduate from college with the ability to assist business in the identification and implementation of industry standards. Before information systems students are able to help businesses manage risks associated with accepting credit cards, and before other students in our core information systems classes enter the workplace, it is important to first educate them about the PCI DSS requirements [22] prior to a focus on technologies such as tokenization that retailers use or end-to-end encryption or challenges like network segmentation that retailers face in order to meet PCI DSS requirements [15].

The 12 PCI DSS requirements, developed in 2004 cover the need for businesses to have a secure network, protect cardholder data, maintain a vulnerability management program, have strong access control measures and monitor and test networks, and have an information security policy. According to a study conducted by Verizon [Verizon 2011], which examined compliance experiences of over 500 businesses in 2010, some requirements are more difficult for businesses to comply with than others and show lower rates of compliance (see Table 1 below).

This paper presents a study that examines students' perceptions of the PCI DSS requirements. Specifically, a ranking exercise showed what students thought about the difficulties business face when complying with the 12 requirements in the PCI DSS. Student rankings were compared to realities faced by businesses as in a manner not uncommon to research which examines what students perceive as difficult and compares it to what faculty perceive as difficult concepts in a course [20]. The ranking exercise also supports the principles of constructivist epistemology.

Table 1: PCI Requirement Compliance Sorted By Difficulty of Compliance from Low to High

PCI DSS Requirement	2010	Categorization as Low, Moderate or High Difficulty for Business Compliance
7. Restrict access to data by business need-to-know	75%	Low Difficulty
4. Encrypt transmission of cardholder data and sensitive information across public networks	72%	Low Difficulty
5. Use and regularly update anti-virus software	64%	Low Difficulty
2. Do not use vendor-supplied defaults for system passwords and other security parameters	56%	Low Difficulty
9. Restrict physical access to cardholder data	55%	Moderate Difficulty
6. Develop and maintain secure systems and applications	53%	Moderate Difficulty
10. Track and monitor all access to network resources and cardholder data	52%	Moderate Difficulty
8. Assign a unique ID to each person with computer access	47%	Moderate Difficulty
1. Install and maintain a firewall configuration to protect data	44%	High Difficulty
3. Protect stored data	42%	High Difficulty
12. Maintain a policy that addresses information security	39%	High Difficulty
11. Regularly test security systems and processes	37%	High Difficulty

USING INDUSTRY STANDARDS

Use of Standards in College Classrooms

Students working with industry standards, such as those for the retail card payment industry, PCI DSS, are given the chance to better understand the real-world difficulties retail businesses face when accepting credit cards payments. Such tasks in the classroom will make students more aware of their role in helping businesses navigate their way through compliance with industry standards and avoid the risks associated with non-compliance. Students familiar with industry standards gain real-world knowledge in the industries in which they plan to one day work. Several different types of standards are being used in post-secondary education in a wide range of disciplines from accounting to software engineering [12, 13, 17]. In accounting, for example, using current accounting standards helps students understand changing global practices. The Securities and Exchange Commission (SEC) is expected to switch from Generally Accepted Accounting principles (GAAP) to International Financial Reporting Standards (IFRS) within the next decade. It is critical to teach those standards in the classroom so students become familiar with global industry practices [13].

Even though the use of standards occurs in a variety of disciplines, it is often found in software engineering and information systems classrooms. The use of standards in the classroom can be classified in several different ways: standards can be included in vocational or university settings; students can interact with standards at the graduate or undergraduate level; standards can be modified or unmodified; and standards can be developed by industries or corporations. For example, the corporate Nokia OK application standards are being used with software engineering students at Auburn University to better prepare them for potential employment [29]. Nokia designed the Nokia OK application standards as a guide to programming wireless devices. Besides corporate standards, industry standards such as the ISO standards, for example, have also been used in information security classes.

Research also demonstrates that standards have been used in the college classroom at the vocational, undergraduate and graduate levels. For example standards such as the IT life cycle processes (ISO12207) have been used in doctoral level IT courses to give a baseline framework for explaining how the software lifecycle works [26]. On the other end of the spectrum, standards have frequently been used in undergraduate programs, such as students using the corporate Nokia OK application standards [29] and software engineering students using the Unified Process standards better understand programming [12]. Besides using standards in university level classes, standards are also important to include at the vocational and community college level. Many technical-level jobs require the use of standards and industry requires entry-level candidates to be knowledgeable in the applicable standards [33].

Several barriers to the use of industry standards in the classroom can arise. The first is that students may not be at a level where they can fully grasp the complexities of the standards often due to their length. For example, the security standards for federal information systems published by the National Institute of Standards and Technology are over 400 pages long [19] which can be unsuitable to use in a typical semester. When standards are overly long or complex, it is possible to rewrite those standards for a more user-friendly version. For example, the corporate Nokia OK application standards were modified both to remove references specific to Nokia and to simplify the standards by removing overly-technical language [29]. Another constraint could be the actual cost of obtaining the industry standards for classroom use. It might be possible to overcome this issue through library purchases of standards that are then made available for classroom use [28].

Payment Card Industry Data Security Standard

Fortunately, PCI DSS is at a level of complexity that college students can understand, so the noted barriers to using industry standards in the classroom are not at play when using PCI DSS requirements. Rather, most of the requirements are straight forward and involve concepts already familiar to college students. PCI DSS requirements were developed as a joint venture between major credit card companies: American Express, Visa, MasterCard, Discover and JCB. While overall data security is involved in the standard, the protection of card holder data, securing account numbers and access codes, are the key to the protection efforts [16]. The Payment Card Industry Council serves as an oversight board and coordinates the development of modified standards, a process that involves all the card company members.

The failure to comply with the PCI DSS requirements has serious consequences for businesses. Under the contractual agreement that binds the business to the PCI DSS requirements, noncompliance can result in fines, increased transaction fees or ouster from the card payment system [23]. The federal government also investigates and acts against businesses not in compliance with the PCI DSS requirements when a data breach occurs. Actions of the Federal Trade Commission, established under the Federal Trade Commission Act, demonstrate that the agency deems non-compliance with the PCI DSS requirements to be an unfair and deceptive trade practice [9]. Several states, including Minnesota and Nevada have enacted statutes using the PCI DSS requirements as the legal standard for data security in the card payment industry [18, 21].The legal issues associated with not complying with PCI DSS standards contribute to the incorporation of the standards into the classroom being a worthwhile activity.

How would student responses to the PCI DSS requirements compare to the business response?

In order to find out what students perceived regarding the implementation of the PCI DSS requirements, students were asked to rank the requirements according to their how difficult they thought it was for businesses to comply. This active learning activity exposes students to industry standards, calls on them to consider what they already know about data security, and requires them to explore the concept further. Understanding student perceptions before creating activities ideally results in more appropriate activities to help students better understand small businesses and the security requirements they face in order to accept credit card payments. This method of exposing students to industry standards also supports a constructivist approach to learning.

Constructivism and Active Learning

Active learning is a significant component of an epistemological philosophy called constructivism, the basis of which is the concept that knowledge is acquired in a process that involves the construction of new knowledge onto preexisting knowledge and experiences [30]. Students, then, can gain and acquire knowledge of data security requirements by building on preexisting knowledge and experiences they already have in that area. By definition, constructivism is an active method of learning that is dependent on the student's interaction with new material rather than on traditional classroom lectures. Learning is not focused on teaching; rather learning is a student-centered process that is self-directed [14]. Educators guide students by providing opportunities for examining preexisting knowledge in light of new information [27].

Certainly, students do come into the information systems classroom with their own perception of what data security means and how businesses apply security concepts. They use passwords and usernames to protect online accounts which contain information deemed private and/or sensitive [10]. Student experiences also expand to some knowledge of security risks; the media supplies students with tales of identity theft and data breaches [4, 11]. When students enter a classroom in which they will study a variety of information systems topics, security will already be a familiar term. However, each individual's background and experience will differ so, in accordance with a constructivist approach, each student is permitted to explore his or her own knowledge with real-world problems [1]. This process also allows educators to get a glimpse of where students stand as to knowledge students have already acquired [24].

The use of the PCI DSS requirements to introduce and study data security also promotes the application of knowledge of situations the students will face in their futures. Some knowledge of payment card industry data security standards are needed for all those entering business, not just those whose careers will be in information systems. The security requirements ranking activity provides exposure to the demands of marketplace and enables students to form connections between classroom and workplace [14].

RESEARCH METHODOLOGY

In order to understand student perceptions of difficulties businesses face when implementing PCI DSS requirements, students were asked, in a survey, to rank six of the PCI DSS requirements from 1 (least difficult for businesses to implement) to 6 (most difficult for businesses to implement) using each number only once. No teacher-structured activity was conducted prior to the ranking activity that students were given.

The following procedure was used to create the two sets of requirements to be ranked: first, the requirements from the Verizon Payment Card Industry study [31] were coded as low difficulty, moderate difficulty or high difficulty based on the percent of organizations meeting that requirement. For example, the requirement that deals with encrypting cardholder data (Requirement 4) showed an implementation rate of 72% and would thus be categorized as low difficulty whereas the requirement dealing with testing security systems regularly (Requirement 11) showed an implementation rate of 37% and would be categorized as high difficulty (see Table 2).

Next, a random number generator was used to create two random sets with the following characteristics: the first set, called the *High Difficulty Set*, contained one requirement considered low difficulty (Requirement 4), two moderately difficult requirements (Requirements 8 and 9), and three requirements in the high difficulty category (Requirements 1, 3 and 12); the second set, called the *Low Difficulty Set*, contained three requirements considered low difficulty (Requirements 2, 5, and 7), two moderately difficult requirements (Requirements 6 and 10) and one requirement in the high difficulty category (Requirement 11). To understand the extent to which students understand the difficulties businesses face when accepting credit cards, the following hypothesis was tested:

H_1: There will be significant differences in the rankings students give to requirements categorized as *low difficulty* compared to the items categorized as *high difficulty*

RESULTS

Surveys were administered to two sections of a core information systems class taken by all business majors. Of the 48 students who took the survey, 39 completed it, with male students comprising 56% of the sample while female students comprised 44%.

For both the *Low Difficulty Set* and the *High Difficulty Set* described above, nonparametric Friedman tests [6] were used to determine whether students thought some PCI requirements were more difficult for businesses to implement than other requirements (see Table 2 on the following page).

There were statistically significant differences in student perceptions of difficulties that businesses would have in implementing PCI DSS requirements for both the *Low Difficulty Set*, $\chi^2(5) = 36.306$, $p < .0001$, and for the *High Difficulty Set*, $\chi^2(5) = 20.156$, $p = .001$. Post hoc analysis using a Wilcoxon signed-rank tests, with a Bonferroni correction applied resulting level of significance at $p < 0.017$, were conducted to determine whether students ranked requirements categorized as low difficulty differently than they did requirements categorized as high difficulty. For the *Low Difficulty Set*, there were no significant differences between requirement 11 and requirement 5 ($Z = -.846$, $p = .398$) or between Requirement 11 and Requirement 2 ($Z = -.772$, $p = .440$), students did perceive requirement 11 as more difficult to implement compared to Requirement 7 ($Z = -2.871$, $p = .004$). For the *High Difficulty Set*, there were no significant differences between Requirement 4 and Requirement 1 ($Z = -1.836$, $p = .066$) or between Requirement 4 and Requirement 3 ($Z = -1.591$, $p = .112$), or between requirement 4 and requirement 12 ($Z = -2.045$, $p = .041$).

Table 2. Means for Student Rankings of PCI DSS Requirements in the Low and High Difficulty Sets

	N	M	SD
Low Difficulty Set of PCI Requirements			
Requirement 5: Use and regularly update anti-virus software	18	2.06	1.259
Requirement 11: Regularly test security systems and processes	18	2.39	1.145
Requirement 2: Do not use vendor-supplied defaults for system passwords	18	2.94	1.662
Requirement 7: Restrict access to data by business need-to-know	18	3.89	1.323
Requirement 10: Track and monitor all access to network resources and cardholder data	18	4.22	1.592
Requirement 6: Develop and maintain secure systems and applications	18	5.11	1.183
High Difficulty Set of PCI Requirements			
Requirement 8: Assign a unique ID to each person with computer access	21	2.24	1.578
Requirement 9: Restrict physical access to cardholder data	21	3.19	1.470
Requirement 12: Maintain a policy that addresses information security	21	3.29	1.707
Requirement 1: Install and maintain a firewall configuration to protect data	21	3.62	1.687
Requirement 3: Protect stored data	21	4.00	1.414
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks	21	4.67	1.183

Assigning ranks to the Verizon Study data [31] based on the percent compliance and comparing these ranks to student perceptions of compliance difficulty indicate that there are PCI DSS requirements where there is disagreement (see Figure 1 on the following page). For example, while companies in the Verizon study found easy to comply with Requirement 4 (Encrypt transmission of Cardholder data) and Requirement 7 (Restrict Access to Data Based on Business Need to Know), students thought both of those requirements would be much more difficult to implement. Conversely, while businesses found it more difficult to comply with Requirement 11 (Regularly Test Security Systems and Processes) and Requirement 12 (Maintain an Information Security Policy), students thought those requirements would be less difficult to comply with.

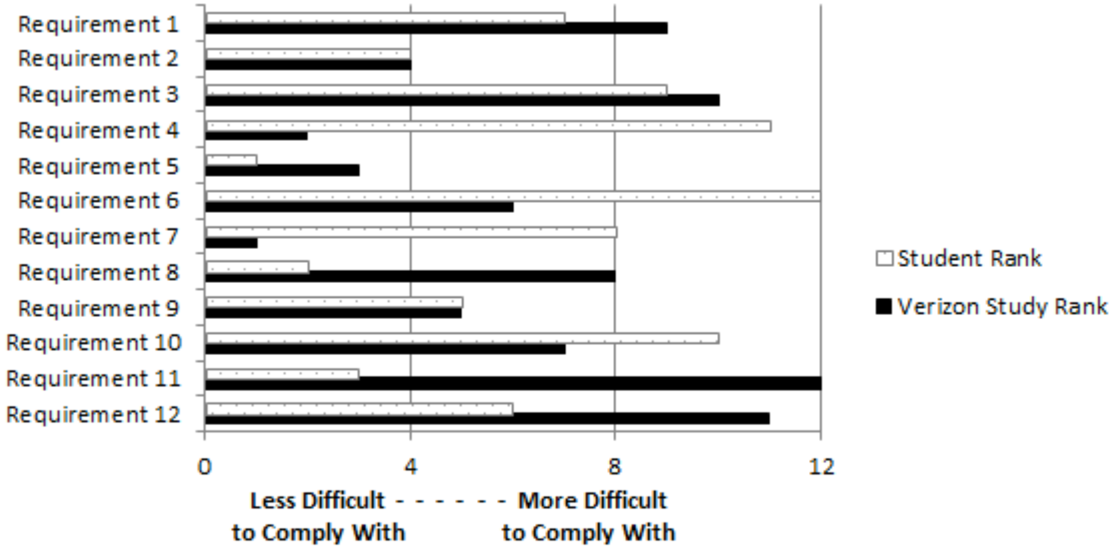

Figure1: Comparison of Ranks of the 12 PCI DSS Requirements

CONCLUSIONS

While it is not entirely surprising that student perceptions of the abilities to comply with the 12 PCI DSS requirements differ from the experiences of businesses going through the compliance process, it is nonetheless quite interesting. It is possible that students find Requirement 4, concerning encrypting the transmission of cardholder data across public networks, difficult because students don't understand the word *encryption* or don't understand the process of encryption. Researchers have suggested that if we don't understand something, such as a process or product, it might be that we consider it difficult because that which we don't understand is an innovation [5], and certainly, this occurs in the realm of technology quite often; however, though encryption techniques evolve, the concept itself would likely not be considered an innovation per se. Another recent study [20] showed that college students found concepts such as the Fourier Transform difficult precisely because they didn't understand the computational steps involved and had a difficult time connecting steps in a process to a concept. A related reason students found the Fourier Transform concept difficult was because they "got lost" in the mathematical symbols.

Besides not understanding a concept because it may be innovative or students may not understand the steps involved in the process or the symbols that represent the concepts, students might also find something difficult because of the vocabulary used. Language, like math and artificial systems, has syntax and utilizes symbols [2] which may be difficult for students to understand. It has long been known that when students don't know the vocabulary words in a sentence, they have difficulty understanding what they read [3]. For example, Davis [7] examined nine reading skills and showed that for college students, word knowledge plays a critical role in reading comprehension noting that "to read at all it is necessary to recognize words and to recall their meanings," (p. 191). A later study [8] utilizing a cross-validated uniqueness analysis using multiple survey forms found that in tests of reading comprehension, nearly a third (32%) of the unique variance associated with word recognition was unique among the eight skills examined in the study which included such skills as being able to follow the structure of a passage, identify techniques used by writers, recognize an author's attitude, tone, mood or purpose, draw inferences from a passage and find answer to questions. This lack of comprehension may contribute to the perceptions that students have regarding it being difficult for businesses to comply with. Much like students might consider that which they don't understand to be difficult, students might, on the other hand, consider that which they do understand to be easy. It may be that students perceived that Requirement 12 (maintaining an information security policy) and Requirement 11 (regularly testing security systems and processes) would be easier for businesses to comply with because the students themselves are familiar with the concept of a having a test to determine success and familiar with policies. Even so, student experience with policies has more than likely provided them with policies that are easier to maintain (no parking, no smoking, no hat, no shoes, no service) than typical corporate policies which are often broader and certainly leave room for interpretation.

This research represents a first step in a longer constructive process that starts with understanding what students perceive about PCI DSS requirements and business compliance. First, future research is in order to better understand why students think encryption is difficult for businesses to comply with and why they think regularly testing systems and maintaining information security policies are easier for businesses to comply with. Later, future research is in order to measure the effectiveness of activities and learning experiences we create to help students in core management information systems classes better relate to business realities where information security involving credit cards are concerned. It is clear that we have our work cut out for as we attempt to align our students' thinking with the experiences of businesses by adding to our students' current knowledge of information security by building new knowledge constructively.

REFERENCES

1. Airasian, P. and Walsh, M. (1997). Constructivist Cautions, 78 *Phi Delta Kappan*, 444- 447.
2. Cangelosi, A. (2001). Evolution of communication and language using signals, symbols, and words. Evolutionary Computation. *IEEE Transactions on Evolution Computation*, 5(2), 93-101.
3. Blachowicz, C., Fisher, P., Ogle, D., & Watts-Taffe, S. (2006). Vocabulary: Questions from the classroom. *Reading Research Quarterly, 41*(4), 524-539.
4. Brown, R. (2012). South Carolina Offers Details of Data Theft and Warns It Could Happen Elsewhere. Available: www.nytimes.com/2012/11/21/us/more-details-of-south-carolina-hacking-episode.html?ref=identityfraud
5. Cho, H., & Schwarz, N. (2006). If I don't understand it, it must be new: Processing fluency and perceived product innovativeness. *Advances in Consumer Research*, *33*, 319.
6. Conover, W. J. (1999). Practical Nonparametric Statistics, 3rd Edition. John Wiley Sons, Inc.: New York.
7. Davis, F. B. (1944). Fundamental factors of comprehension in reading. *Psychometrika*, *9*(3), 185-197.
8. Davis, F. B. (1968). Research in comprehension in reading. *Reading Research Quarterly*, 499-545.
9. Federal Trade Commission Act, Section 5, (15 U.S.C. §45).
10. Florencio, D. and Herley, C (2007). A Large-Scale Study of Web Password Habits. Microsoft Research. Available: http://research.microsoft.com/pubs/74164/www2007.pdf.
11. Greenberg, A. (2013). Video Service Vudu Resets Users' Passwords after Burglars Steal Its Hard Drives. Available: http://www.forbes.com/sites/andygreenberg/2013/04/09/video-service-vudu-resets-users-passwords-after-burglars-steal-its-hard-drives/.
12. Halling, M., Zuser, W., Kohle, M., & Biffl, S. (2002). Teaching the unified process to undergraduate students. In Software Engineering Education and Training, 2002.(CSEE&T 2002). Proceedings. 15th Conference on (pp. 148-159). IEEE.
13. James, M. (2011). Integrating international financial reporting standards into the accounting curriculum: Strategies, benefits and challenges. *Academy of Educational Leadership Journal, 15*, S127-S142.
14. Kumar, M. (2006). Constructivist Epistemology in Action. *Journal of Educational Thought, 40*(3), 247-261.

15. Litan, A. (2011). Gartner Survey: Challenged U.S. firms seek alternative PCI-compliance solutions. Available: http://www.gartner.com/id=1733430
16. MacCarthy, M. (2011). Information Security Policy in the U.S. Retail Payments Industry. *Stanford Technology Law Review,* 3-35.
17. Meyer, B. (2001). Software engineering in the academy. *Computer*, *34*(5), 28-35.
18. Minn. Stat. Ann §365E.64(2) (2007).
19. National Institute of Standards and Technology (2013). Security and Privacy Controls for Federal Information Systems and Organizations, 1-457. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
20. Nelson, J. K., Hjalmarson, M. A., Wage, K. E., & Buck, J. R. (2010, October). Students' interpretation of the importance and difficulty of concepts in signals and systems. In *Frontiers in Education Conference (FIE), 2010 IEEE* (T3G-1-T3G6). IEEE.
21. Nev. Rev. Stat. §603A.215 (2010).
22. Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures, version 2.0 (2010). Available: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf
23. Rees, J. (2012). Tackling the PCI DSS Challenges, *Computer Fraud &Security*, 2012(1), 215-217.
24. Sewell, A. (2002). Constructivism and Student Misconceptions. *Australian Science Teachers Journal, 48*(4), 24-28.
25. Statistics of U.S. Businesses (SUSB) Main. Available: http://www.census.gov/econ/susb/.
26. Steenkamp, A. L., & Van, D. J. (2004). An approach to teaching it life cycle processes. In Proceedings of ISECON (21).
27. Swortzel, K. (1999). Constructivism: The Career and Technical Education Perspective. *Journal of Vocational and Technical Education, 16*(1). Available: http://scholar.lib.vt.edu/ejournals/JVTE/v16n1/doolittle.html
28. Traynor, B. (2011, October). Usability standards—Evolution, access and practice. In Professional Communication Conference (IPCC), 2011 IEEE International, 1-8.
29. Umphress, D. A., Cross II, J. H., Jain, J., Meda, N., & Barowski, L. A. (2004). Bringing J2ME industry practice into the classroom. *ACM SIGCSE Bulletin, 36*(1), 301-305.
30. von Glaserfeld, E. (1989). Cognition, *Construction of Knowledge and Teaching*, 80 Synthese, 121-140.
31. Verizon (2011). Verizon 2011 PCI Compliance Report (2011). Available: http://www.verizonenterprise.com/resources/reports/rp_2011-payment-card-industry-compliance-report_en_xg.pdf?__ct_return=1
32. Verizon (2012). 2012 Data Breach Investigations Report. Available: http://www.verizonenterprise.com/DBIR/2012/
33. Zinser, R., & Lawrenz, F. (2004). New roles to meet industry needs: A look at the advanced technological education program. *Journal of Vocational Education Research, 29*(2), 85-99.