https://doi.org/10.48009/2_iis_2020_270-278

Issues in Information Systems

Volume 21, Issue 2, pp. 270-278, 2020

PERSONAL EFFECTIVENESS COMPETENCIES OF RECENT CYBERSECURITY GRADUATES

Nelbert "Doc" St. Clair, College of Coastal Georgia, nstclair@ccga.edu
John Girard, Middle Georgia State University, john.girard@mga.edu

ABSTRACT

This article highlights the findings of a study that surveyed employers' and professors' expectations of recent cybersecurity graduates in the workforce. The focus of this article is the personal effectiveness competencies (interpersonal skills, integrity, professionalism, initiative, adaptability and flexibility, dependability and reliability, and lifelong learning) that are expected by employers when cybersecurity graduates are hired. The major finding was the unanticipated discovery of a statistically significant difference for integrity ($t = 2.56$, $p < .01$) between professionals and professors.

Keywords: Cybersecurity, Education, Competencies, Personal, and Effectiveness

INTRODUCTION

The term "cybersecurity" is becoming a well-known word in today's lexicon (Manyika & Roxburgh, 2011). With the Internet's ability to share and disseminate knowledge, organizational consumers or users such as the media have increased their ability to quickly assemble, transmit, or disseminate information without haste. This expediency has superseded time, space, and undue process to educate individuals on evolving current news stories about high-profile security breaches. Viral transmissions have created a cultural phenomenon in the industry to heighten public awareness about the vulnerabilities of the Internet and cybercrimes, such as data breaches and cybersecurity threats (Manyika & Roxburgh, 2011).

The number of cybercrimes is escalating each year, with the U.S.–based companies being targeted by hackers who seek to obtain, sell, embarrass or trade information. According to Internet Crime Complaint Center (IC3), the number of complaints on cybercrime received as of 2016 had grown from 168,400 in 2000 to 269,422 by 2014 (2014 Internet Crime Report, 2016). The trading of data or information encapsulates such things as personal data, patents, intellectual property rights, movies, and the latest research and development projects at innovative companies. Retailers, high-tech firms, entertainment companies, and U.S. federal government agencies are investing in safeguards to ward off cyber-crimes (2014 Internet Crime Report, 2016).

Since 2000, the IC3 has received complaints crossing the spectrum of cybercrime matters, to include online fraud in its different forms including Intellectual Property Rights (IPR) matters, Computer Intrusions (hacking), Economic Espionage (Theft of Trade Secrets), Online Extortion, International Money Laundering, Identity Theft, and a growing list of Internet-facilitated crimes. It has become increasingly evident that, regardless of the label placed on a cybercrime matter, the potential for it to overlap with another referred matter is substantial. Therefore, the IC3, formerly known as the Internet Fraud Complaint Center (Internet Fraud Complaint Center), was renamed in October 2003 to better reflect the broad character of such matters having an Internet, or cyber, nexus referred to the IC3, and to minimize the need for one to distinguish "Internet Fraud" from other potentially overlapping cybercrimes. (About IC3, 2016, p. 1). Therefore, the demand for cybersecurity professionals is growing at a phenomenal rate.

The main focus of this study is to explore the personal effectiveness competencies employers' desire from recent cybersecurity graduates in the United States. For the purpose of this study, a recent cybersecurity graduate is defined as a person who graduated from a college or university with a degree in cybersecurity or information security within two years.

LITERATURE REVIEW

One way to address academic and professional competencies is through the use of competency models. Competency is defined as a group of core knowledge, skill, and abilities that are assigned to a job. These competencies are used to

measure job performance and aide in annual work review reports (Parry, 1998). Additionally, competency models have been used by business and industries, for over 40 years, to help qualify individuals to fill jobs (Ennis, 2015). In the early 1970s, McClelland found these "competencies" were a significant predictor of performance and success in the workplace (McClelland, 1973; Lucia & Lepsinger, 1999). Lucia and Lepsinger (1999) determined a person's academic aptitude and academic performance is just as important as competencies. Other researchers have found competency is a whole person and not one-dimension factor.

The U.S. Department of Labor, Employment and Training Administration (ETA), periodically publishes competency models to assist employers in identifying emerging needs (Bureau of Labor Statistics, U.S. Department of Labor, 2015). One of the largest concerns facing ETA is the looming retirements of the "Baby Boomer" generation, and the gap they will leave in the workforce. These Baby Boomers, who were born between 1946 and 1964, are currently retired or looking into retirement options. Because of this, the ETA has involved academic institutions, employers, industries, and training leaders in order to develop different competency models (Ennis, 2015).

In June of 2014, Cybersecurity Competency Model (CSCM) was released by The Employment and Training Administration (ETA). The model has a specific purpose:

> [It was] designed to represent the competencies needed by individuals whose activities impact the security of their organization's cyberspace. These include both the average worker who uses their organization's computer network or Internet as well as the cybersecurity professionals and network administrators. (Cybersecurity Competency Model, 2015, p. 3).

The CSCM, as shown in
Figure 1, has a total of five tiers, with each tier covering a different group of competencies. The number of competencies can range from seven to nine per tier, depending on the needs of the employer and the environment of the employee (Shippman, et al., 2000). Foundational Competencies for this model are Tiers 1 to 3. These competencies are most commonly known as "soft-skills," which are the "non-technical" skills, abilities and traits that one needs to function in a specific employment environment. Tadimeti (2014) characterizes workplace "non-technical" skills as, "problem-solving, cognitive skills, oral communication skills, personal qualities, work ethics, interpersonal and teamwork" (Tadimeti, 2014, p. 34).

Figure 1. Cybersecurity competency model (Cybersecurity Competency Model, 2015).

Tier 1, which is the main focus of this article, addresses soft skills and research shows that recent graduates are not aware of the needs for soft skills when applying for a job ((Moss & Tilly, 1996; Murti, 2014). However, employers require employees to have these sets of soft skills and they can use this model to help determine if a potential employee fits their organizational culture. The common term for this is known as a "good fit." This term, "good fit" does not

look at technical skills (Moss & Tilly, 1996). The CCSM places the following competencies in Tier 1: interpersonal skills, integrity, professionalism, initiative, adaptability and flexibility, dependability and reliability, and lifelong learning. For Tier 1, "Personal Effectiveness Competencies are personal attributes essential for all life roles. Personal effectiveness competencies are generally learned in the home or community and honed at school and in the workplace" (DOL, 2014, p. 6).

METHODOLOGY

The purpose of this project was to identify personal effectiveness competencies employers expect from recent cybersecurity graduates and to determine if there is an expectation gap between the current cyber curriculum and those of employers when they hire cybersecurity graduates. Specifically, this research involved surveying a sample of 104 cybersecurity professionals and 44 faculty members in the United States. The first survey determined the core competencies employers expected from recent cybersecurity graduates. The second survey identified if there is a disconnect between what is being taught in cybersecurity curriculum and industry's knowledge demands.

For the purpose of this study, a recent cybersecurity graduate is defined as someone who graduated from a college or university, with a degree in cybersecurity or information security, within the last two years. This definition encouraged participants to focus on recent graduates and not those who have been in the field longer.

Research Design

A quantitative methodology was selected for this research. The quantitative method was selected after reviewing the literature and discovering models used by past scholars. This project utilizes the research design of Kavanagh and Drennan (2008), Kesner (2008), and Treadwell and Treadwell (1999). The designs were modified to aid in the collection and analysis of data on the employers' expectations. Additionally, Paullet's (2009) double survey approach to collect and analyze data was incorporated into the design with the scholar's permission. Paullet's method captured the experiences between two different populations. Thus, two different surveys were administered.

Cybersecurity professionals and professors were the two populations that participated in the research project, with each group being located within the United States. Meanwhile, cybersecurity professionals—the first population—consisted of those who were employed in the cybersecurity industry or supervised cybersecurity professionals. The sources of respondents were the Metro Atlanta Chapter of ISSA, LinkedIn profiles, and the snowballing technique for reaching out to colleagues with whom the researcher worked with in the past. The second population sample came from any faculty member who taught cybersecurity courses at the higher education institutions within the United States. The technique of snowballing was used to reach out to other colleagues in academia who taught cybersecurity courses from different higher education institutions. The first survey was administered to 104 cybersecurity professionals and the second survey was administered to 44 cybersecurity professors.

Survey Instrument

An original survey instrument was developed for the study by using the cybersecurity competency model released in June 2014. This model was created by industry professionals and academic professors to help shape the knowledge of other cybersecurity professionals. Some employers can also use this model to help create a more detailed job description for a future cybersecurity employee. The model was designed with five different levels. The survey instrument was designed to determine what skill sets employers expect from recent cybersecurity graduates. The survey consisted of 11 structured questions, and one open-ended question to provide an opportunity for additional comments from the participants. Open-ended questions were designed to collect narrative responses that participants wanted to add to the data collection (Nardi, 2014).

The first part of both the professional and professor survey instruments included demographics and classification questions. The main part of the survey was divided into five questions; with each question having subtopics in which the participant was asked to rate the sub-competency areas. These five questions consisted of a 5-point Likert scale, in which participants were asked to rate competencies as very important, important, neutral, less important, or not important. The two surveys provided different questions depending on who, Professional (Pro) or Professor (Prof),

took the survey. The two surveys provided different questions depending on who, Professional (Pro) or Professor (Prof), took the survey. The forced responses choices were the same.

As shown in Figure 2, the questions used the categories, such as "Personal Effectiveness Competencies," from the Cybersecurity Competency Model (CSCM), without specifically referencing the model.

Professional: How important are _____ when hiring or working with recent cyber security graduates?

Professor: How important do you think it is to incorporate the following _____ into the curriculum when teaching cyber security courses?

Figure 2. Example question for professional and professor

This article focuses on the responses related to the Personal Effectiveness Competencies (see Figure 3). The instrument included one question that pertained to "personal attributes essential for all life roles. Often referred to as soft skills, personal effectiveness competencies were generally learned in the home or community and honed at school and in the workplace" (DOL, 2014, p. 6).

Personal Effectiveness Competencies are personal attributes essential for all life roles. Often referred to as "soft skills," personal effectiveness competencies are generally learned in the home or community and honed at school and in the workplace.

Professional: How important are Personal Effectiveness Competencies when hiring or working with recent cyber security graduates?

Professor: How important do you think it is to incorporate the following Personal Effectiveness Competencies into the curriculum when teaching cyber security courses?

	Very Important	Important	Neutral	Less Important	Not Important
Interpersonal Skills	❑	❑	❑	❑	❑
Integrity	❑	❑	❑	❑	❑
Professionalism	❑	❑	❑	❑	❑
Initiative	❑	❑	❑	❑	❑
Adaptability and Flexibility	❑	❑	❑	❑	❑
Dependability and Reliability	❑	❑	❑	❑	❑
Lifelong Learning	❑	❑	❑	❑	❑

Figure 3. Personal effectiveness competencies.

The last question of this survey was open-ended (see Figure 4). The purpose of this question was to capture any ideas, thoughts, or responses that were not available to the participants in the previous questions (Nardi, 2014).

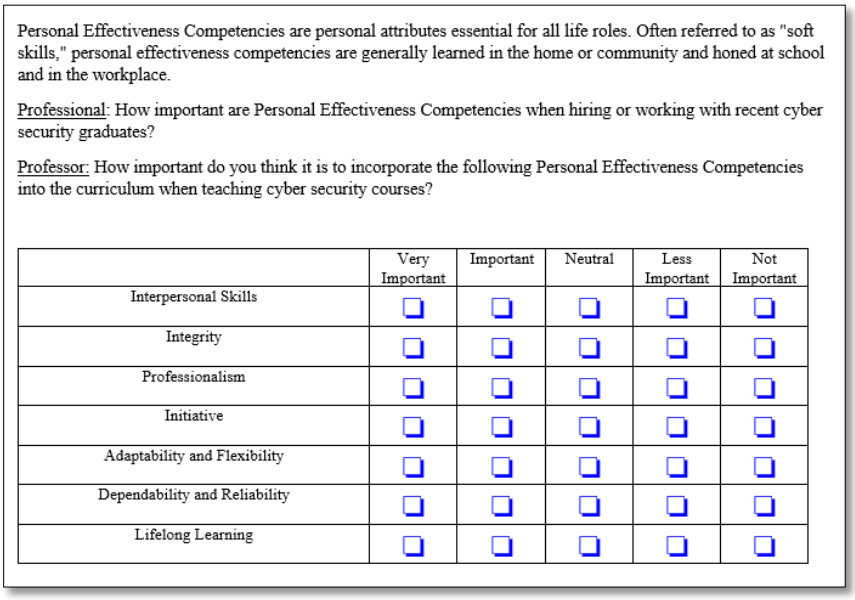
Professional: From your experience/perspective, what competencies do you expect recent cyber security graduate(s) to have on the first day of employment?

Professor: From your experience/perspective, what recommendations would you suggest to improve quality and integrity of the current cybersecurity curriculum or course(s) you teach?

Figure 4. Open-ended question.

Data Analysis Plan

The participants were presented with the equivalent survey, but their questions were phrased differently, depending on which survey was given. The questions were phrased differently so that the participants would be able to understand or interpret given their experience in whether they were a professional or a professor. Figure 5 shows the difference between the two surveys as it related to the questions.



Personal Effectiveness Competencies are personal attributes essential for all life roles. Often referred to as "soft skills," personal effectiveness competencies are generally learned in the home or community and honed at school and in the workplace.

Professional: How important are Personal Effectiveness Competencies when hiring or working with recent cyber security graduates?

Professor: How important do you think it is to incorporate the following Personal Effectiveness Competencies into the curriculum when teaching cyber security courses?

	Very Important	Important	Neutral	Less Important	Not Important
Interpersonal Skills	❑	❑	❑	❑	❑
Integrity	❑	❑	❑	❑	❑
Professionalism	❑	❑	❑	❑	❑
Initiative	❑	❑	❑	❑	❑
Adaptability and Flexibility	❑	❑	❑	❑	❑
Dependability and Reliability	❑	❑	❑	❑	❑
Lifelong Learning	❑	❑	❑	❑	❑

Figure 5. Shows the different type of survey questions

Question Pro was used to collect the data. The data were analyzed through SPSS for statistical data, mean, confidence interval, standard deviation, and standard error for each question. Throughout the analysis, SPSS was utilized to generate two-tailed *t* test on questions from the professional and professor surveys. The *t* tests were used to explore the differences and or similarities between groups. The two-tailed *t* test was chosen because of parametric methods appropriate for examining the difference in means between two different populations. The *t* tests are best used when there are "two different (independent) groups of people and one is interested in comparing their scores" (Pallant, 2013, p. 109). The two-tailed *t* test displayed if there was a significant difference in *p* value. If there was a significant difference, based on the traditional value (less than .05), the researcher disclosed and explained this to the readers (Pallant, 2013).

ANALYSIS AND RESULTS

The surveys focused on the relative importance of particular competencies that employers use during the hiring processes for recent cybersecurity graduates. The U.S. Department of Labor's (DOL) Cybersecurity Competency Model (CSCM), which has been available since June 2014, was the basis for both surveys. The model was "designed to represent the competencies needed by individuals whose activities impact the security of their organization's cyberspace. These include both the average worker who uses the Internet or their organization's computer network, as well as entry-level cybersecurity professionals" (Bureau of Labor Statistics, U.S. Department of Labor, 2015, p. 3). Table 1 (Professional) and Table 2 (Professor) show the overall results on personal effectiveness competencies. Personal effectiveness competencies "are personal attributes essential for all life roles. Often referred to as 'soft skills", personal effectiveness competencies are generally learned in the home or community and honed at school and in the workplace" (DOL, 2014, p. 4).

Table 1. Professional: Personal Effectiveness Competencies Breakdown

Pro – Personal Effectiveness Competencies	**Very Important**		**Important**		**Neutral**		**Less Important**		**Not Important**
	%	N	%	N	%	N	%	N	
Interpersonal Skills	50%	53	43%	45	5%	5	2%	2	
Integrity	78%	82	19%	20	3%	3			
Professionalism	64%	67	35%	37	1%	1			
Initiative	63%	66	35%	37	2%	2			
Adaptability and Flexibility	61%	64	38%	40	1%	1			
Dependability and Reliability	80%	84	20%	21					
Lifelong Learning	52%	55	38%	40	9%	9	1%	1	

Table 2. Professor: Personal Effectiveness Competencies Breakdown

Prof – Personal Effectiveness Competencies	**Very Important**		**Important**		**Neutral**		**Less Important**		**Not Important**
	%	N	%	N	%	N	%	N	
Interpersonal Skills	70%	31	23%	10	7%	3			
Integrity	96%	42	2%	1	2%	1			
Professionalism	80%	35	16%	7	5%	2			
Initiative	57%	25	32%	14	9%	4	2%	1	
Adaptability and Flexibility	68%	30	25%	11	5%	2	2%	1	
Dependability and Reliability	84%	37	16%	7					
Lifelong Learning	59%	26	36%	16	5%	2			

To determine the differences between professionals and professors, as it relates to personal effectiveness competencies, a two-tailed *t* test was conducted. This test was used to compare if any differences exist between two different groups. As shown in Table 3, the results for personal effectiveness competencies revealed a statistically significant difference for integrity ($t = 2.56$, $p < .01$) between the two groups. A frequency analysis indicated that 95% of the professors and 78% of the professionals agreed that integrity is very important, while 19% of the professionals believed that integrity is important and 2% of the professors agreed. This finding is consistent with the conclusion of Kavanagh and Drennan (2008) that recent graduates lack the soft skills needed in the workforce. They stated it "is unrealistic for universities to attempt to guarantee that graduates will possess the necessary generic skills to meet the demands of employers" (Kavanagh & Drennan, 2008, p. 282) (McCabe, Trevino, & Butterfield, 2001) (McCabe, Trevino, & Butterfield, 2001), meaning not all cybersecurity graduates will have the necessary soft skills to function in the workplace.

This analysis of Personal Effectiveness Competencies helps to answer the question, What are the core competencies employers' expecting from cybersecurity graduates? Because it helps employers hire entry-level cybersecurity professionals by providing a deeper look at the first tier of the model to evaluate a potential new employee based on their soft skills. In addition, answering the question, What core competencies are identified in a cybersecurity program's curriculum that correlate with employers' expectations? What is important to Industry Professionals and Academics because it allows university curricula to meet the needs of the employer by adding modules into the course to support the needs of the employer. This validates the U.S. Department of Labor's Cybersecurity Competency Model

(CSCM) as a good tool for academia and industry to use when developing cybersecurity curricula and evaluating new graduates.

Table 3. Personal Effectiveness Competencies for Professionals and Professors

***t* Test Result – Personal Effectiveness Competencies**	***p***	**Result**
Interpersonal Skills	.059	The result is not significant at p < .05
Integrity	.011	The result is significant at p < .05
Professionalism	.200	The result is not significant at p < .05
Initiative	.162	The result is not significant at p < .05
Adaptability and Flexibility	.938	The result is not significant at p < .05
Dependability and Reliability	.550	The result is not significant at p < .05
Lifelong Learning	.260	The result is not significant at p < .05

DISCUSSION AND CONCLUSION

The statistically significant differences between the professionals and professors regarding integrity was not anticipated. In fact, the expectation was that both groups would rate integrity as "very important" and not have differing opinions in this area. Even though the number of participants in each group was different, the data showed a deep disparity in the percentage of respondents who rated integrity as very important. The fact that 96% professors deemed integrity very important, and statistically significant as compared with professionals, demanded additional analysis to explain this finding.

Toward an Understanding of the Difference

The researchers launched an additional review of the literature to explain the reported differences. To be clear, both groups indicated that integrity is imperative, with 98% of professors selecting important or very important and 97% of professionals selecting important or very important. The area of most interest is the finding of statistically significant difference for integrity ($t = 2.56$, $p < .01$) between the two groups. In essence the question becomes why professors might view the importance of integrity so differently than professionals?

The literature is rich with examples of academic dishonesty and integrity issues. The purpose of this section is not to summarize the literature but rather highlight some reasons why the statistically significant difference between professionals and professors may exist. The researchers hope this will be the catalyst for future research to further the explain the difference. The researchers' own experiences suggest professors regularly deal with academic dishonesty and integrity issues. Today it is commonplace to find a statement on plagiarism or some other form of academic dishonesty in course syllabi. College and universities have policies and procedures in place to discourage such activities and most have aggressive awareness campaigns in place to highlight the possible consequences. Nevertheless, academic dishonesty is part of American higher education.

McCabe et al (2001, p. 219) remind us that this is not a new phenomenon and that "This research demonstrates that cheating is prevalent and that some forms of cheating has increased dramatically in the last 30 years." While trying to answer the question *Why Do College Students Cheat?* Simkin and McLeod (2012) determined that about 60% of business students (and 64% of non-business students) cheated. In a study conducted by Jordan (2001) 55% of students were classified as cheaters. Other researchers suggest there might be a link between cheating and other concerning behaviors. For example, Blankenship & Whitely (2000, p. 8) wrote "The results of this study provided evidence that academic dishonesty has a significant relation with other forms of deviance. One implication of these results is that honesty or dishonesty may be part of a stable dimension of behavior." Aasheim, Rutner, , Lixin Li, & Williams (2012, p. 306), who studied plagiarism in programming classes believe that faculty should do more to help educate students on academic dishonesty and suggested " one way to address the issue is for faculty to hold classroom discussions about academic dishonesty as it relates to programming assignments."

Interestingly, Molnar, Kletke & Chongwatpol (Molnar, Kletke, & Chongwatpol, 2008) suggest technology may play a role in academic dishonestly. They reported that "It appears that in terms of intellectual property violations, undergraduate students in general find cheating using IT more acceptable than cheating without the use of IT. It also appears that undergraduate students perceive that it is relatively more acceptable for them to personally cheat when using IT than for others to cheat when using IT, although this is reversed when IT is not involved." (Molnar, Kletke, & Chongwatpol, 2008, p. 657) Given the close relationship between technology and cybersecurity education, the findings of Molnar et al, may go some way in explaining the difference in level of importance as reported by professors and professionals.

Conclusion

From these studies, we may summarize that cheating is commonplace, many students lack integrity, technology may facilitate integrity breaches, and that this may be part of a student's behavior. Collectively these factors paint a worrying picture of the graduates that professors are sending to the field and therefore may explain the high importance placed on integrity in cybersecurity education. There is much more to learn about integrity and its importance in cybersecurity education. The recommended next step is to refine the reasons why professors and professionals view the importance of integrity so differently.

REFERENCES

2014 Internet Crime Report. (2016, May 10). Retrieved from FederalBureau of Investigation Internet Crime Complaint Center: https://www.ic3.gov/default.aspx

Aasheim, C. L., Rutner, P. S., Lixin, L., & Williams, S. R. (2012). Plagiarism and Programming: A Survey of Student Attitudes. *Journal of Information Systems Education, 23*(3), 297-313.

About IC3. (2016, June 6). Retrieved from Federal Bureau Of Investigation Internet Crime Complaint Center (IC3): https://www.ic3.gov/about/default.aspx

Blankenship, K. L. (2000). Relation of General Deviance to Academic Dishonesty. *Ethics & Behavior, 10*(1), 1-12.

Bureau of Labor Statistics, U.S. Department of Labor. (2015, January 25). Retrieved from Occupational Outlook Handbook, 2014-15 Edition, Information Security Analysts,: http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6

Campbell, K. S. (2014). *Manufacturing Workforce Development Playbook.* Chicago: Summit Media Group, Inc. .

Cybersecurity Competency Model. (2015, January 4). Retrieved from Competency Model Clearinghouse: http://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx

DOL. (2014). *Cybersecurity Competency Model*. Retrieved from CareerOneStop (DOL): http://www.careeronestop.org/CompetencyModel/competency-models/cybersecurity.aspx

Ennis, M. R. (2015, March 1). *Competency Models: A Review of the Literature and the Role of the Employment and Training Administration (ETA).* Retrieved from U.S. Department of Labor, Employment and Training Administration: http://www.careeronestop.org/CompetencyModel/Info_Documents/OPDRLiteratureReview.pdf

Jordan, A. E. (2001). College Student Cheating: The Role of Motivation, Perceived Norms, Attitudes, and Knowledge of Institutional Policy. *Ethics & Behavior, 11*(3), 233-247.

Kavanagh, M. H., & Drennan, L. (2008). What skills and attributes does an accounting graduate need? Evidence from student perceptions and employer expectations. *Accounting & Finance, 48(2)*, 279-300.

Kesner, R. M. (2008). Business School Undergraduate Information Management Competencies: A Study of Employer Expectations and Associated Curricular Recommendations. *Communications Of The Association For Information Systems, 23*, 633-654.

Lucia, A. D., & Lepsinger, R. (1999). The art and science of competency models: Pinpointing critical success factors in organizations. *New York: Pfeiffer*.

Manyika, J., & Roxburgh, C. (2011, October). *The great transformer: The impact of the Internet on economic growth and prosperity*. Retrieved from McKinsey & Company: http://www.mckinsey.com/industries/high-tech/our-insights/the-great-transformer

McCabe, D., Trevino, L. K., & Butterfield, K. (2001). Cheating in Academic Institutions: A Decade of Research. *Ethics & Behavior, 11*(3), 219-232.

McClelland, D. C. (1973). Testing for competence rather than for intelligence. *American Psychologist, 28*, 1-14.

McClelland, D. C. (1998). Identifying competencies with behavioral-event interviews. *American Psychologist, 9(5)*, 339.

Molnar, K. K., Kletke, M. G., & Chongwatpol, J. (2008). thics vs. IT Ethics: Do Undergraduate Students Perceive a Difference? . *Journal of Business Ethics, 83*(4), 657-671.

Moss, P., & Tilly, C. (1996). Soft' Skills and Race: An Investigation of Black Men's. *Work and Occupations, Vol. 23, No. 3*, 252-276.

Murti, A. B. (2014). Why Soft Skills Matter. *IUP Journal Of Soft Skills, 8(3)*, 32-36.

Nardi, P. M. (2014). *Doing Survey Research: A guide to quantitative Methods.* Boulder: Paradigm.

Pallant, J. (2013). *SPSS Survival Manual: A Step by Step Guide to Data Analysis Using IBM Spss, 5th edition.* Boston: Open University Press .

Parry, S. B. (1998). Just what is a competency? (and why should you care?). *Training, 35(6)*, 58-64.

Paullet, K. L. (2009, July 16). An exploratory study of cyberstalking: Students and law enforcement in Allegheny county, Pennsylvania.

Shippman, J. S., Ash, , R. A., Battista, M., Carr, L., Eyde, L. D., Hesketh, B., . . . Sanchez, J. I. (2000). The practice of competency modeling. *Personnel Psychology, 53*, 703-740.

Simkin, M. G., & McLeod, A. (2012). Plagiarism and Programming: A Survey of Student Attitudes. *Journal of Information Systems Education, 23*(3), 297-313.

Tadimeti, V. (2014). E-Soft Skills Training: Challenges and Opportunities. *IUP Journal Of Soft Skills, 8(1)*, 34-44.

Treadwell, D. F., & Treadwell, J. B. (1999). Employer Expectations of Newly-Hired Communication Graduates. *Journal Of The Association For Communication Administration 28, no. 2*, 87-99.