https://doi.org/10.48009/3_iis_2018_193-201

Issues in Information Systems
Volume 19, Issue 3, pp. 193-201, 2018

CYBERSECURITY CERTIFICATIONS MATTER

Jason E. James, Sullivan University, jejames@sullivan.edu
Jennifer Callen, PNC Bank, Jennifer.callen@pnc.com

ABSTRACT

Technology advancements are moving faster than we can keep pace. These advancements are naturally shortening the amount of time that information is accurate and useful before it is replaced by new knowledge. Since this knowledge/information gap exists, there is a desire to define and implement industry mechanisms that allow professionals to acquire new knowledge, skills, and abilities to forge successful careers. Such mechanisms enable professionals the ability to keep pace with the constant changing technological landscape, such as information security where the demand for effectively educated individuals is growing exponentially. As we continue to create advancements in technology and further shorten the viable life of information, the greater the need to identify strategies that will support individuals as they transition into high tech careers. (Hayward, 2014) Years ago, having an undergraduate education and/or an advanced education was suffice. Today companies are requiring IT professionals to obtain and maintain professional certifications as a requirement to hire and keep their jobs.

Keywords: Certifications, Cybersecurity, Education, Professional, and Information Technology

INTRODUCTION

The growth of IT and rapid advancement of cybersecurity has resulted in the demand for workers with specialized skills and has placed a considerable demand on the traditional educational system to provide a qualified and sustainable cybersecurity workforce (Randle & Zirkle, 2005). In response to advances in computer technology, rapidly depreciating skill sets, and the slow response of traditional education, the IT industry uses certification as a way to train and accredit the workforce (Clarke, 2001). Cantor (2002) defines certification "as a confirmation of one's adequate knowledge and skills in a specified occupation or occupational specialty." Further, Cantor classifies cybersecurity certifications into two areas: (1) certifications issued by industry that are product-related and (2) certifications issued by organizations or professional associations.

In 1989, Novell created the first IT certification in response to a lack of trained individuals to support their mission critical tasks and the inability to turn to the traditional educational system for a trained supply of workers (Ziob, 2000). IT certifications, particularly cybersecurity, have since grown as a result of the need for the IT industry to support its products and services. (Randle & Zirkle, 2005). A 2013 (ISC)2 Global Information Security Workforce Study and the National Academy of Science report: Professionalizing the Nation's Cyber security Workforce (2013), demonstrated that there was a lack of qualified information security individuals necessary to meet future demands, and the gap between qualified professionals and demand will continue to be high and increase over time. The lack of skilled and qualified cybersecurity professionals has always been a major issue and industry certification has been seen as a mechanism to fill those "gaps" in knowledge as identified by industry workforce studies. (Hayward, 2014)

The lack of skilled and qualified cybersecurity professionals has always been an issue in the IT industry. Is there really a need for cybersecurity certification to qualify for a job and does it really help? The rapid pace at which technology continues to evolve, creates a need for highly skilled individuals to enable, apply, support, configure, and adapt IT products and services (Randle & Zirkle, 2005). Because cybersecurity certifications represent a standard measurement for specific skills, companies are seeking out professionals with these credentials (Al-Rawi, Lansari, & Bouslama, 2005). Cybersecurity certification programs are considered by many to be responsive to industry needs and providing up-to-date, relevant training for continuously changing skill sets. Industry-based cybersecurity certifications have become a standard precursor to employment for many job roles serving as an indication to human resource managers that specific knowledge or competencies have been met. Cybersecurity certification is thought to provide a verification of skills and knowledge related to a broad or specific type of technology, hardware, software, or IT product (Randle

& Zirkle, 2005).

Certification matters for three reasons:

1. Confidence – certification preparation assures well-trained cybersecurity professionals they are more confident and the skills they possess are appropriate and useful for their responsibilities
2. Validation - reliably attests to the level of knowledge and certified professionals can be relied on to perform at a higher level and have more knowledge than untrained employees
3. Execution - performance of important business activities is more assuring with certified professionals and they can be expected to perform assigned tasks more consistently, thus increasing reliability and overall organizational execution (Cybersecurity Credentials Collaborative, 2015)

The purpose of this qualitative multiple holistic case study was to explore if there is really a need for cybersecurity certification to qualify for a job and if it really helps. This study was part of a bigger study to explore the importance of partnerships between higher education and professional cybersecurity associations for the field of cybersecurity. That study explored how partnerships can impact the knowledge, skills, and abilities of students and the likelihood of a successful career in the cybersecurity workforce the partnerships can provide. This study explored how certifications can impact the likelihood of a successful career in the cybersecurity workforce. In order determine the importance of certifications; research was conducted in one professional cybersecurity association within Central Indiana and multiple higher education institutions within Indiana.

LITERATURE REVIEW

The purpose of the literature review was to examine the existing literature to determine how the lack of skilled and qualified cybersecurity professionals has always been an issue in the IT industry and if there is really a need for cybersecurity certification to qualify for a job and if it really helps. Therefore, the review of the literature focused on cybersecurity literature related to certifications and cybersecurity job requirements.

Despite the rapid abundance of cybersecurity certification programs as an industry standard, there is no consensus as to whether certification improves workplace performance. However, evidence does suggest that certifications raise competence in fields that have certification standards (Andersson, 2009). In addition, voluntary professional cybersecurity certifications are used as indicators of professional skill (Jenkins, 2005). Professional associations such as the Computing Technology Industry Association (CompTIA), International Council of Electronic Commerce Consultants (EC-Council), Global Information Assurance Certification (GIAC), ISACA, and The International Information Systems Security Certification Consortium ((ISC)²) (Cybersecurity Credentials Collaborative (C3), 2015) comprise 7 out of the top 12 vendor-neutral cybersecurity certifications by salary and thus will be within scope of this study (Certification Magazine, 2015). The remaining five are vendor-specific certifications, which will not be covered in this research study. The seven certifications included in this study include ISACA's Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), and Certified Information Systems Auditor (CISA); (ISC)2's Certified Information Systems Security Professional (CISSP); GIAC's Certified Incident Handler; EC-Council's Certified Ethical Hacker (CEH); and CompTIA's Security+ (Certification Magazine, 2015).

CompTIA is a non-profit trade association, dedicated to advancing the global interests of cybersecurity professionals. CompTIA provides cybersecurity education, certifications, business credentials, and resources as well as networking opportunities for professionals to connect with like-minded, leading cybersecurity industry experts (Capella University, 2015).

EC-Council is a member-supported professional organization providing cybersecurity resources for professionals in the field. Certifications offered include those focusing on disaster recovery, ethical hacking, secure programming, forensic investigation, and more (Capella University, 2015).

GIAC was founded in 1999 with a mission to provide relevant certifications that serve to validate the skills of cybersecurity professionals. GIAC certifications are awarded in key areas of computer, information and software security and address a range of skill sets including entry-level and broad-based cybersecurity essentials. Targeted

certification focus on subject areas such as audit, forensics, hacking, incident response, and more (Capella University, 2015).

ISACA, formerly known as Information Systems Audit and Control Association, but now goes by just the acronym, is an independent, nonprofit organization that provides practical guidance and certification programs for cybersecurity professionals in all career stages (Capella University, 2015).

(ISC)2 offers education and certification programs for cybersecurity professionals in all career stages. With a membership of over 100,000, (ISC)² provides access to a large network of industry professionals worldwide (Capella University, 2015).

Industry experts point out several advantages to having professional credentials and certification. Walter McFarland, former executive at Booz Allen Hamilton, offered two compelling reasons why cybersecurity professionals should contemplate advancing their credentials. First, credentialing meets increasing demands for continuous development and second, seeking certification enhances marketability (Davenport, 2006). A minority of higher education institutions recognized this early on for their students, combining cybersecurity certifications with degree offerings and acting as agents of both vendor-specific and vendor-neutral IT training (Adelman, 2000). A further advantage to credentialing is that professional certifications are one of the defining characteristics of a profession. Specifically, McFarland stated that, "A hallmark of any profession is its ability to articulate the body of knowledge that defines it. Certification is demonstrated mastery of that specific body of knowledge" (Davenport, 2006). Professional certification enhances the status of the field. In addition, hiring managers view job candidates with certifications as more productive and cybersecurity certifications enhance a candidate's credibility during job interviews (Andersson, 2009).

A cybersecurity professional can learn knowledge and expertise through multiple years of education, such as an undergraduate and graduate degree in cybersecurity, but it does not mean the individual knows how to apply the learned knowledge with a high level of skill. Therefore, certifications are necessary so that employers do not necessarily have to rely on references or go through several candidates to determine if an individual is really an expert cybersecurity professional (Sager, 1995). Certifications are an excellent way for individuals to apply their knowledge within a minimum level (Cegielski, 2008). Certification is a method of estimation of an individual's expertise via a standardized measurement instrument, such as a standardized exam, (Cegielski, 2004) in which an individual must meet a minimum level to qualify as an expert in the field of cybersecurity. Typically, a professional cybersecurity association who sponsors a certification determines the expert knowledge threshold (Sager, 1995) and therefore, companies are able to make decisions when trying to select an expert through using professional certifications to narrow the choice of candidates (Cegielski, 2008).

As far as the world of cybersecurity, professionals should have expertise in five knowledge domains; availability, authentication, integrity, confidentiality, and non-repudiation. Finally, just as a certified public accountants (CPA) and lawyer (bar) have formal methods of estimation of expertise through exams, so should cybersecurity professionals. However, unlike the CPA and bar exams utilized by the public accounting and legal profession, the world of cybersecurity is so broad in scope that no single assessment of expertise exists. Rather, cybersecurity professionals prove expertise in a specific field of cybersecurity and obtain credentials through passing one of several examinations in the industry such as the CISA exam or the CISSP exam (Cegielski, 2008).

Cybersecurity professionals are not the only beneficiaries of cybersecurity certifications, companies' benefit through improved employee recruitment, development, and retention while higher education institutions improve both curriculum content and assessment capabilities. As for cybersecurity professionals, they obtain the following benefits that come with certification:

- Support - obtaining certifications via exams provide valid measurements of competencies,
- Marketability - content of field of study considered valuable by potential employers,
- Financial - potential employers relate certification to proof of knowledge, skills, and abilities and reward with higher salaries (Ray & McCoy, 2000).

Cybersecurity professionals who increase their knowledge, skills, and abilities through certification are more valuable

employees to companies as it proves their strength (Martinez, 1999). In fact, research has shown the benefits of certified employees include: increased knowledge, greater productivity, higher level of skill and expertise, reduced training costs, and higher morale and commitment (Ray & McCoy, 2000)

With all that said, four-year higher education institutions have been slow to offer cybersecurity students the benefit of a certification to complement their degrees. However, that trend has been changing and integrating certification programs into traditional coursework provides better-quality employer prospects and increases a cybersecurity student's chance of higher salary and long-lasting career with a good company (Randall & Zirkle, 2005).

METHODOLOGY

This study did not involve a survey, but instead used open-ended interviews as the main source of data collection. The reason is that research through surveys attempts to find frequencies in answers as well as a distribution of traits in the sampled population. Open-ended interviews attempt to find specific themes for research questions. The current study involved a multiple descriptive case study methodology that performed empirical research to discover facts about the need for cybersecurity certification to qualify for a job and if it really helps. The sampling is the study used 12 participants total, 6 different cybersecurity faculties and 6 different cybersecurity professionals. All the participants are part of the researcher's professional network.

The research study was conducted in one professional cybersecurity association and multiple higher education institutions because they represent a major segment of cybersecurity professionals and experts in their field. Participant selection was accomplished through the process of purposeful sampling. In qualitative research, the intent is not to generalize to a population, but to develop an in-depth exploration of a central phenomenon. The criteria used for maximum variation sampling for this research study for participants was that the professional cybersecurity professionals have at least 10 years' cybersecurity experience and do not work for the same company and cybersecurity faculty must currently teach cybersecurity classes at a higher education institution.

The current research study involved an interview guide administered through in-person interviews. The interview instrument allowed for a broader range of responses as compared to a set number of alternatives used with standard surveys. The goal was to gather responses from each of the purposeful sample of members. The interview guide allowed participants to articulate if there is really a need for cybersecurity certification to qualify for a job and if it really helps.

DATA ANALYSIS

Since this was a multiple holistic case study, the research relied on multiple sources of evidence, (Yin, 2014) and collected using three methods: semi-structured interviews, documentation, and direct observation. However, the majority of the data for this research was obtained through interviews with the study participants. The nature of the information sought in this study - assumptions, beliefs, expectations, and experiences - could not be adequately gathered through direct observation and documents alone, thus making the majority of the data gathered from one-on-one interviews with cybersecurity professionals and faculty interviews, the most appropriate method of data collection. (Collins, 1998).

In beginning the coding process, the answers to the interview questions were examined for consistency. Specific words or phrases were noted and counted for frequency. The purpose of this technique was to discover common themes and patterns in the responses to learn common answers to specific questions. The researcher manually went through each interview to code specific words and themes throughout all answers for a particular question. The coding words were then organized with in tables to give a visual representation of the themes. The tables provided for a more hands-on, manual approach that allowed for an in-depth analysis of the coding process as each question was examined for consistency across all participants. From this raw data, the analysis aimed to generate overall themes and answer the research questions (Gall, Gall, & Borg, 2003).

During the course of the 12 in-person interviews, one of many interview questions were administered in a consistent manner, however only two were relevant to this study as identified below. No pilot tests were performed because the interview guide was already previously established by an earlier study (Collins, 1998) with their permission. As a vital part of the research, the participants were asked to provide their input to the following interview questions:

IQ1 What do you perceive is the impact (pros and cons) on the knowledge, skills, and abilities of cybersecurity students when a relationship exists between cybersecurity professionals and higher education institutions?
IQ2 What do you perceive are the benefits (drawbacks) on their career in the cybersecurity workforce when a relationship exists?
Significant answers to the questions were identified for both cybersecurity professionals and cybersecurity faculty and noted as such in order to establish the context for the themes that were identified. The main themes from the interviews of the cybersecurity professionals are identified in the following table:

Table 1. Themes from interviews of Cybersecurity Professionals for IQ1

Themes	Number of References
Access to Cybersecurity Professionals	1
Lots of Resources	1
Networking	1
Real life experience	5
Teach and Real World Needed	1
Time Consuming (Negative)	1
Training	1

One of the key responses came from participant, who said, "the purpose of an academic setting is to teach students content. The purpose of professional associations is designed to allow them to engage with people who have real world experience. Those are two very different pieces of the educational puzzle. Real world experience, in my opinion, is what allows the student to assimilate into their knowledge base. How to really perform their job. So I don't think you can do one without the other. That's why in the late '90s, in the early '2000s you heard so much about paper certs because people would just go and memorize a bunch of stuff and get certifications. It had no real solid reflection of their job skill abilities. Where being involved with a professional association gives you the opportunity to be surrounded by, and work with other more experienced professionals to help you simulate that information in your own knowledge base."
Cybersecurity faculty had a much broader view for IQ1 and the main themes from the interviews with the participants included the following table:

Table 2. Themes from interviews of Cybersecurity Faculty for IQ1

Themes	**Number of References**	**Industry Experience**
Acquire multitude of cybersecurity knowledge & skills	1	Yes
Certifications	1	Yes
Cyber competitions	1	Yes
Cybersecurity knowledge beyond classroom	1	Yes
Journal Publications	1	Yes
Learn from Cybersecurity Professionals	3	Yes
Attain meaningful careers	1	Yes
Network	2	Yes
Real world experience beyond classroom	1	Yes
Teach and real world needed	1	Yes
Up-to-date knowledge on cybersecurity trends	1	Yes
Relationship building for cybersecurity knowledge & skills	1	No
Internships	1	No
Practical experience	1	No
Technology research & development	1	No
Cheap admission conferences	1	No
Minority benefits for women/foreigners	1	No
Class work, research, access peer groups at meetings	1	No
Network, journals, access to electronics library	1	No
Research conferences	1	No

One of the best responses came from a participant who said that "not having those relationship is -- to me, devastating and believe that they are inhibitive to the students because the more that the students are exposed to cyber security professionals, the better equipped they're going to be, and the more they're going to be able to interact and network and learn skills of those knowledge skills and abilities from professionals and more tools for their toolbox. In other words, they're going to be able to learn more. We teach a set curriculum, and we try to teach as much as we can, but we know that that curriculum is just a small bit in that bucket of knowledge that exists out there."

The second interview question for the study, what do you perceive are the benefits (drawbacks) on their career in the cybersecurity workforce when a relationship exists, resulted in the following main themes from the cybersecurity professionals and are identified in the following table:

Table 3. Themes from interviews of Cybersecurity Professionals for IQ2

Themes	Number of References
Certifications	1
Curriculum but no real life experience	1
Develop personal relationships	1
Industry and Real World Practices	1
Internships	1
Mentor/Mentee	1
Networking, Expertise, Job opportunities	2
Professional association help build career path	1
Ready access to professionals	1
Recommendation and endorsement	1
Broaden horizon, too focused on one aspect of cybersecurity	1

One of the key responses came from participant who said, "actually the benefit is that again you get that chance to meet people that are currently doing that career or have the hiring decision for it helps to already form some of personal relationship with that person and hopefully they have internships. Companies want students with experience and the students just don't have real life experience. They have the curriculum that they need and they have the education but they don't have that real life experience in themselves. I think it portrays to the students that, if they get involved, they have a really good chance of maybe getting a job right out of college".

Cybersecurity faculty themes were much the same as cybersecurity professionals as some of the same themes seem to come up in their responses as seen in the following table:

Table 4. Themes from interviews of Cybersecurity Faculty for IQ2

Themes	**Number of References**	**Industry Experience**
Access to webinars	1	Yes
Certifications	2	Yes & No
Cybersecurity professionals provide guidance for careers	1	Yes
Learning governance of organizations	1	Yes
Networking	1	Yes
Professional cybersecurity speakers	1	Yes
Real world experience via internships	2	Yes
Advanced membership advantage for job seeking	1	No
Enhanced expectation for what job will be	1	No
Increase ability to network and find local jobs	1	No
Time and service in professional association	1	No

One of the important responses came from a participant who said "benefits are big since the students would be more knowledgeable, especially about the practical application of standards and processing procedures that organizations need to have in place. It would be better to have some good hands on experience, instead of just the theoretical understanding as a result."

Certifications were mentioned 4 different times during the interviews. The results of the analysis confirmed there was a unanimous agreement between cybersecurity professionals and cybersecurity faculty and is a win-win situation for employers and students. The reason for that unanimous agreement is that cybersecurity students will increase their knowledge, skills, and abilities while in school and companies would be able to hire more qualified cybersecurity students upon graduation.

DISCUSSION

Students need to learn cybersecurity in the classroom and beyond, no matter what their major, whether it is computer science, information systems, information technology, or cybersecurity. Cybersecurity is an ever-changing field and the only way to keep up is to learn the same way as cybersecurity professionals: training, reading journal publications produced by cybersecurity associations for its members, member only webinars, and of course, certifications. The types of cybersecurity training in and beyond the classroom is often overlooked in cybersecurity education and is a great informal learning environment that can be related closely to academic objectives. Cybersecurity certifications and corresponding training can provide those types of learning's and increase a cybersecurity students knowledge, skills, and abilities and give them an edge when applying to jobs (Ramey-Gassert, 1997).

Cybersecurity graduates compete in a global market fueled by rapid innovation and constant technological advances. In order to be able to contribute to and advance in this highly demanding and lucrative career, cybersecurity students not only require advanced scientific and technological knowledge but they also need the knowledge, skills, and abilities needed in the career. These competencies can be found and enhanced through co-curricular activities, such as cybersecurity training, competitions, journal publications, webinars, seminars, and of course, certifications (Starr & Minchella, 2016).

While employers state that college graduates are ready for entry-level jobs, they add that they lack the knowledge, skills and abilities they need in order to advance within a company. A report from the Association of American Colleges and Universities questioned "whether graduates are in fact achieving the level of preparation—in terms of knowledge, capabilities, and personal qualities—that will enable them to both thrive and contribute in a fast changing economy and in turbulent, highly demanding global, societal, and often personal contexts" (Schneider, 2008, p. 2).

CONCLUSION

College students today need, expect, and deserve more than intense learning than just in a classroom and textbooks. In order to attain "great jobs and great lives," they require high impact experiences inside and outside the classroom that open up opportunities, reveal options, and develop flexibility. Certifications can provide cybersecurity students such experiences. Students have the opportunity to learn beyond the classroom and collaborate with others in settings populated by people from different backgrounds and demographic groups. They make sense of experiences by reflecting on the resources gained and their applicability to their future careers. In summary, cybersecurity certifications can broaden and deepen cybersecurity student learning by promoting a linkage between learning in the classroom and beyond. It helps ensure that graduates gain the knowledge, skills, and abilities that both cybersecurity professionals and cybersecurity faculties agreed could provide and prepare students for the complex and volatile world of the twenty-first century. By obtaining certifications, value is added to their degrees and obtaining jobs in the field becomes much easier (Starr & Minchella, 2016).

REFERENCES

Adelman, C. (2000). A parallel universe. *Change* (32), 20-29. Retrieved from http://search.proquest.com/docview/208052014?accountid=28365.

Andersson, D. L. (2009, April). *Information technology industry certification's impact on undergraduate student perception of instructor effectiveness.* Retrieved October 24, 2015, from ProQuest Dissertations & Theses Global: https://reddog.rmu.edu/login?url=http://search.proquest.com/docview/305177281?accountid=28365

Al-Rawi, A., Lansari, A., & Bouslama, F. (2005). Integrating Sun certification objectives in to an IS programming course. *The Journal of Issues in Informing Science and Information Technology, 2*, 247- 257. Retrieved February 15, 2017 from http://www.proceedings.informingscience.org/InSITE2005/I20f39Rawi.pdf

Cantor, J. (2002). Skills certifications and workforce development: Partnering with industry and ourselves. Leadership Abstracts, 15 (1). Retrieved February 15, 2017, from https://eric.ed.gov/?id=ED481380

Capella University. (2015, July 30). *Professional organizations in information security*. Retrieved December 4, 2015, from Information Security Career Central: http://www.capella.edu/infosec/professional-organizations/

Cegielski, C. G. (2008). Toward the development of an interdisciplinary information assurance curriculum: Knowledge domains and skill sets required of information assurance professionals. *Decision Sciences Journal of Innovative Education, 6*(1), 29-49 Retrieved October 27, 2015 from https://reddog.rmu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ehh&AN=29383947&site=eds-live&scope=site

Cegielski, C. G. (2004). Who values technology certification? *Communications of the ACM , 47* (10), 103-105 Retrieved November 11, 2015 from EBSCOhost: https://reddog.rmu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=14523209&site=eds-live&scope=site.

Certification Magazine. (2015, November 18). *Salary survey PLUS: Cybersecurity certs = big money*. Retrieved November 25, 2015, from Certification Magazine: http://certmag.com/salary-survey-plus-cybersecurity-certs-big-money/

Clarke, B. (2001, July). Corporate curricula in schools: issues and implementation. Paper presented at the meeting of the Seventh World Conference on Computers in Education, Copenhagen, Denmark.

Collins, M. M. (1998, May). *Exploring professional associations' perceptions of institutions of higher education as potential partners.* Retrieved January 18, 2015, from ProQuest Dissertations & Theses Global: https://reddog.rmu.edu/login?url=http://search.proquest.com/docview/304443794?accountid=28365

Cybersecurity Credentials Collaborative (C3). (2015, October). *Why Certification Matters - Analysis of the Value of IT Certification.* Retrieved November 24, 2015, from Cybersecurity Credentials Collaborative (C3): http://www.cybersecuritycc.org

Davenport, R. (2006). Credentialing and certification. *T + D, 60*(5), 60-61. Retrieved from http://search.proquest.com/docview/227013079?accountid=28365.

Gall, M., Gall, J., & Borg, W. (2003). *Educational research: An introduction* (7th Edition ed.). New York, New York, Allyn and Bacon.

Hayward, R. (2014). *Certification and education: Cultivating the global workforce landscape*. Retrieved December 22, 2015, from Information System Security Certification Consortium, Inc., (ISC)²: https://isc2.org/uploadedfiles/%28isc%292_public_content/isc2-certification-and-education-white-paper-heyward.pdf

Jenkins, E. J. (2005, May). *Certifications in computer areas: The demand for hiring employees with various certifications. An assessment of the workplace skills desired for placement of Mississippi Community*

College Information Systems Technology completers. Retrieved October 24, 2015, from ProQuest Dissertations & Theses Global: https://reddog.rmu.edu/login?url=http://search.proquest.com/docview/305448595?accountid=28365

Martinez, A. (1999). *Get certified and get ahead: Millennium edition.* New York: McGraw-Hill.

Ramey-Gassert, L. (1997). Learning science beyond the classroom. *The Elementary School Journal , 97* (4), 433-450 Retrieved from https://reddog.rmu.edu/login?url=http://reddog.rmu.edu:2077/docview/224524279?accountid=28365.

Randall, M. H., & Zirkle, C. J. (2005). Information technology student-based certification in formal education settings: Who benefits and what are needed. *Journal of Information Technology Education, 4*, 287-306 Retrieved on October 27, 2015 from https://reddog.rmu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ehh&AN=19763457&site=eds-live&scope=site.

Ray, C. M., & McCoy, R. (2000). Why certification in information systems? *Information Technology, Learning, and Performance Journal, 18*(1), Retrieved October 21, 2015 from ProQuest Central: https://reddog.rmu.edu/login?url=http://search.proquest.com/docview/219816410?accountid=28365

Sager, W. H. (1995). Characteristics of a profession. *The National Public Accountant, 40*(3), 6 Retrieved November 11, 2015 from ProQuest Central:https://reddog.rmu.edu/login?url=http://search.proquest.com/docview/232358962?accountid=28365

Schneider, C. (2008). *Introduction: Liberal Education and High-Impact Practices: A Brief Overview. In G. Kuh, High-Impact Educational Practices: What They Are, Who Has Access to Them, and Why They Matter.* Association of American Colleges and Universities. Sweitzer, E.

Starr, L., & Minchella, D. (2016). Learning beyond the science classroom: A roadmap to success. *Journal of STEM Education: Innovations and Research, 17*(1), 52-57 Retrieved from https://reddog.rmu.edu/login?url=http://reddog.rmu.edu:2077/docview/1785759031?accountid=28365 .

Yin, R. K. (2014). *Case study research: Design and methods* (5th Edition ed.). Thousand Oaks, CA: SAGE Publications.

Ziob, L. L. (2000). Time is flying: 10 years of IT certifications. *Certification Magazine*.