Open Access License Notice

Are Cybersecurity Professionals Satisfied with Recent Cybersecurity Graduates?

Nelbert St. Clair
School of Business and Public Management
College of Coastal Georgia
Brunswick, GA, USA
nstclair@ccga.edu

John Girard
School of Computing
Middle Georgia State University
Macon, GA, USA
john.girard@mga.edu

***Abstract*—This pioneering research project examines the expectations of cybersecurity professionals in terms of contentment with recent graduates. In particular, the project sought to determine the professionals' satisfaction with recent hires of undergraduate graduates. Overall, 73% of the participants indicated satisfaction with recent cybersecurity graduates. In addition, 67% of these professionals believed that recent graduates had a satisfactory level of competency.**

Keywords—cybersecurity, graduates, employer, expectations

I. Background

A background history of the Internet describes how cyber-attacks have evolved. In 1969, ARPANET (Advanced Research Projects Agency Network), a government-funded program, connected four universities: Stanford University's Research Institute, University of California at Los Angeles, University of California at Santa Barbara, and University of Utah [1]. The goal of the project was to design a computer network with the ability to share information without being in the same geographical location [1]. By participating in this project, each university was tasked with linking its independent system (networked computer) with the others. This kinship connection for the academic scholarship was the beginning of the Internet or World Wide Web [1]. This paradoxical adventure in information sharing opened doors for innovation, creativity, and economic advancement in organizations. With every innovation in economies, there are individuals who seek to prosper off another's conceptual models or paradigm-shifting innovations. Thus, with every innovation, there is always an equivalent force in nature recognizing the revolutionary conception; and it is already seeking methods to capitalize on the invention [1].

The Internet's conceptualization did not directly come with criminals intact, but inevitability with various new types of innovation, new criminals are lurking in the shadows [2]. Unfortunately, new laws and regulations passed by both national and state governments have struggled to keep up with the advancement of the Internet, which allow hackers, particularly experienced ones, to stay steps ahead of the judicial process. Cyber or computer crimes existed before the Internet entered the public domain. A computer crime or cybercrime is defined as "criminal activity that involves the use of one or more computers" [2, p. 12]. In 1972, John Draper (aka, Cap' n Crunch) became the first hacker to obtain unauthorized access to the AT&T switching network. Draper discovered, a free toy whistle in a box of Cap' n Crunch cereal, would generate the same frequency needed to gain access to the AT&T long-distance switching system. The actions enabled him to make free long-distance calls. From this discovery, Draper built a device called the blue box. This box could generate a 260 MHz tone, which enabled the user to make free long-distance telephone calls [3].

During the 1970s, the U.S. government addressed cybercrimes as a problem, with the passage of the Federal Computer Systems Protection Act, which defines "computer crimes" and recommends penalties for such crimes [4]. The Act made "it a Federal crime for a person to directly or indirectly access or cause to be accessed for fraudulent purposes a computer system affecting commerce or having a connection with a Federal agency or financial institution" [4, p. 1].

From 2012 to 2015, cyber-attacks have affected millions of people in several organizations, including the Federal Office of Personnel Management (2015), Anthem (2014), Home Depot (2014), and Target (2013; 2014 Internet Crime Report, 2016). Home Depot operates in over 2,200 locations worldwide, and it reported $83.2 billion in sales and $6.3 billion in earnings in 2014. Home Depot was the victim of a cyberattack, where the hackers stole 53 million customer email addresses [5]. This caused concern that hackers would try to obtain personal identification information (PII) by using phishing scams [5]. Phishing is the method of collecting PII from a person by using bogus emails or websites that look legitimate [6]. Office of HIPAA Privacy & Security, (2015) describes PII as follows:

> Any information that can be used to identify, contact, or locate an individual, either alone or combined with other easily accessible sources. It includes information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Examples of data elements that can identify an individual include name, fingerprints or other biometric (including genetic) data, email address, telephone number, or social security number. [7, p. 1]

All Cyber-attacks have "potential economic consequences" and create "uncertainty in business planning

An earlier version of this article earned the Best Paper Award at 23rd Colloquium.

as well as consumer confidence," according to former United States Deputy Assistant Secretary of Transportation for Technology Policy, Dr. Oliver McGee [8, p. 1]. The President of the United States, Barack Obama, addressed the issue of cybercrimes in the 2015 State of the Union address. The President stated hackers seek to steal personal identification information (PII) and sell the information on the black market to whoever is willing to pay for the information. President Obama believes that hackers mean to disrupt our way of life, and stores like Target and Home Depot are easy targets of opportunity. President Obama warned the American public and organizations that they should recognize cyber-attacks as real threats to our society and business during his 2015 State of the Union address [9].

According to former Defense Secretary Chuck Hagel (March 2014), the Pentagon has started to "triple its cybersecurity personnel over the next several years to bolster US national security" [10, p. 1]. In addition, the federal government has been recruiting cyber professionals, creating the "Cyber Corps," a National Science Foundation scholarship grant program. This Program paid tuition for students to become government cybersecurity professionals, as it sought to meet the estimated 6,000 workers needed by the year 2016 [11] [12].

As the demand for cybersecurity professionals increases, educators must find ways to train students to become professionals for the future [13]. President Obama's call to action, Educate to Innovate, has increased national awareness for cyber education. In accordance, K–12, and higher education domains have searched for methods to increase the United States investment in STEM incentives (Science, Technology, Engineering, and Math) by combining government and privately funded programs [14]. The National Initiative for Cybersecurity Education (NICE) offers ways for educators to access resources to help develop curriculums. NICE also encourages the integration of cybersecurity into all subjects [15].

Rubens stated that these security positions are still in demand and that the security skills shortage continues to be unfilled [16]. The scale of the cybersecurity skills shortage described by Rubens is phenomenal as he describes that by the end of 2018, one to two million cyber security jobs will remain open. Rayome outlined the top 5 most in-demand cybersecurity skills. These cybersecurity skills are as follows [17].

1. IT security specialist
2. Information security analyst
3. Network security engineer
4. Security engineer
5. Application security engineer

While examining the current literature, a gap became evident. The literature lacks relevant information that correlates to the expected skill sets cybersecurity graduates ought to have upon graduation, which will be a fundamental area of investigation in this study. It is essential that cybersecurity graduates are informed about the conditions of employment to facilitate becoming a better potential candidate for employment. The purpose of this study was to identify core competencies employers expect from cybersecurity graduates and to determine if there is an expectation gap between the current cyber curriculum and employer expectations when they hire cybersecurity graduates. Explicitly, this research involved surveying a sample of cybersecurity professionals and a group of faculty members in the United States.

II. Literature Review

Ivancevich, Ivancevich, and Roscher conducted research from 26 accounting and recruiting professionals in-order-to gain a better understanding of employer's expectations of the employee's first two years of employment [18]. The researchers used a survey to collect their data and published it in the Certified Public Accountant (CPA) Journal series online. The data were divided into three data sets: (a) Demographic Information, (b) Best Practices During the First Two Years of Employment, and (c) Worst Practices During the First Two Years of Employment. The researchers did not write about how they analyzed the data. The journal article breaks down the data into three different exhibits [18].

First, the demographical information collected was of organization type, position, size of the office, and size of the firm in revenues. The organization type consisted of 20 accounting firms and six others, including industry and government. The positions ranged from campus recruiting to senior accountant/manager. The numbers of respondents were about the same, as it related to the size of the office, the number of employees per office was 51-150 (12 respondents) and > 150 (11 respondents). The size of firm (In Revenues) was as follows: < $750 Million (6), $751 million-$2 Billion (7), > $2 Billion [18].

The second set of data, as shown in the article, Best Practices during the First Two Years of Employment summarized 16 different options [18]. The top three options from the survey were a volunteer for new assignments, being a team player, and showing a desire to learn (12). According to Ivancevich et al. "employers appreciated new hires that showed initiative and were eager for new assignments and additional responsibilities" [18, p. 71]. Employers in the survey demonstrated greater value in employees who were team players and were willing to go beyond their prescribed job descriptions, particularly when it came to volunteerism. Additionally, employers found most rewarding employees had self-motivated, self-starter, and self-learner characteristics. If a new employee could learn new ways and strategies to engage a potential client, this would be beneficial to the organization [18]. The third set of data shown in the article was called Worst Practices during the First Two Years of Employment. The top three options from the survey were "(1) poor work ethics/poor-quality of work, (2) unprofessional behavior, and (3) not a team player / shrinking responsibility" [18].

Treadwell and Treadwell conducted a study about employer's expectations and perceptions of communication among new hires [19]. The study used three defining milestones in a graduate's career as a purpose of the study: (a) the initial job application, (b) the beginning of the first year, and (c) the end of the first year. The goal of the research was to understand how employers would react to recent communication graduates starting from the first contact, which was the application process to his or her first performance review [19]. Treadwell and Treadwell reported the difference sectors surveyed as follows: Higher Education (23.8%); Advertising, Public Relations, Communications, Publishing (17.9%); Finance (11.3%); Medical/Health Care (8.3%); Service Providers (8.3%); "High Tech" (7.7%); Product related (7.7%); and "Other" (13.1%; Treadwell & Treadwell, 1999). The respondents were classified into three categories: as professional communicators or communication managers, human resource administrators, and other managers or professionals [19].

Treadwell and Treadwell's research demonstrated skills lacking by recent graduates, and most importantly, what skills should be developed into an undergraduate curriculum [19] (See Fig. 1). The findings showed writing, grammar, and reporting skills were lacking and critical thinking skills were assessed excessively high, which is a common trait found in the digital higher education culture.

Skills Seen as Lacking by Employers and as Needed in the Undergraduate Curriculum (%)

Skill	Seen as lacking by employers	Should be developed in undergrad curric.
Responsibility (work w/out supervision)	29.8	52.4
Initiative	20.8	47.0
Logical or critical thinking	29.8	69.6
General knowledge, current affairs	21.4	48.8
Writing effectively for multiple audiences	41.1	70.2
Basic writing skills (spelling, grammar)	24.4	67.9
News writing skills	19.0	45.8
Persuasive writing skills, e.g., marketing copy	32.1	58.3
Design skills	21.4	38.1
Other	22.0	21.4

Fig. 1. Skills seen as lacking by employers.

Kavanagh and Drennan stated that employers want recent graduates who have a various set of skills and attributes for accounting. The scholar's research investigated the professional skills students perceived themselves as having at the highlight of their careers. It also attempted to determine what the graduate believed was his or her strongest skill sets. Conversely, the research team looked at the professional skills employers expected from accounting graduates at the start of their careers and the differences between students' perceptions and employer's expectations. The goal of the research was to determine a medium and model for determining what professional skills were important to student's careers [20].

III. Methodology

A survey instrument was developed to gather data form cybersecurity professionals. The first three questions of the survey were related to simple demographics about each individual (see Fig. 2). The participants were asked to self-identify their level of management and to choose the type of organization from the list provided below, with an option to select "other" if their type of organization was not listed. Nardi stated, "The goal of such a survey would simply be to present basic information profiling the respondents" [21]. The first three demographic questions provided the necessary profiling.

1. What is your gender?
   a) Male
   b) Female

2. How would you best describe yourself?
   a) Upper Level Management - For example: CEO, CFO, COO, CTO, CIO, VP, Managing Director
   b) Middle Level Management - For example: Regional, Branch and Departmental Managers, Operational Director
   c) Lower Level Management - For example: Assistant Mangers, Team leader, Foreman, Shift Manager, Supervisor
   d) Individual Contributor (with hiring influence)
   e) Individual Contributor (with NO hiring influence)
   f) Other

3. Which one describes your organization?
   a) Government
   b) Local State
   c) Private
   d) Non-profit
   e) Military
   f) Higher Education
   g) K12
   h) Other

Fig. 2. Questions collecting data on participant demographics.

The fourth and fifth questions (as shown in Fig. 3), addressed supervisors' satisfaction with a recent cybersecurity graduate within their organizations. The fourth question was designed as a filter, which asked the participant if they currently work with or have worked with a recent cybersecurity graduate. The participant's response decided the next question. A response of "yes," determined the fifth question, such as how satisfied are you with a cybersecurity graduate?

4. Do you currently work or supervise personnel in the cyber security industry?
   1. Yes
   2. No

5. Do you currently or have you previously, worked with a recent cyber security graduate(s)?
   a) Yes
   b) No

5a. Overall, how satisfied are you with the recent cyber security graduate(s)?
   a) Very satisfied
   b) Satisfied
   c) Neutral
   d) Dissatisfied
   e) Very dissatisfied

5b. What was your impression of the recent graduate(s) you hired or worked with?

5c. How were they prepared/not prepared for their profession?

Fig. 3. Questions collecting data on supervisors' satisfaction.

979-8-6425-4896-7/20/$26.00 ©2020 CISSE

IV. Data Analysis

A total of 105 cybersecurity professionals completed the survey, giving an 81% participation rate. A total of 129 participants started the survey, but 24 participants did not complete it, perhaps due to survey fatigue or technical difficulties. The participants who did not answer all the questions within the survey were categorized as "withdrew" (See Table I).

TABLE I. Survey Overall Report

Survey Overall Report	Number of Participants
Started	129
Completed	105
Completion Rate	81%
Withdrew	24

As Table II indicates, there was a large difference between the number of male participants, at 87 (82.9%), and female participants, at 18 (17.1%). This shows the fact that in the information technology and information system fields, most employees are males. This finding agrees with other researchers who have studied gender differences within the information technology and information system fields and supports the theory of a male-dominated workforce [22].

TABLE II. Gender Information

What is your gender?	Number of Participants	% of Participants
Male	87	83%
Female	18	17%

Question 2 (Table III) asked the professionals to describe their positions within their organizations. Thirty-five participants (31%) self-identified as middle management, which was the most common answer. An individual contributor, with no hiring influence (24 participants; 22%), was the second most common answer. The third and fourth most common answers were upper-level management, with 19 participants (18%), and individual contributor (with hiring influence), with 17 participants (17%), a one percentage point difference. One participant (1%) selected "other."

TABLE III. Levels of Management Breakdown

How would you best describe yourself?	Number of Participants	% of Participants
Upper Level Management	19	18%
Middle Level Management	35	31%
Lower Level Management	11	11%
Individual Contributor (with hiring influence)	17	17%
Individual Contributor (with NO hiring influence)	22	22%
Other	1	1%

Organizations, from different business sectors, follow different procedures due to the nature of their businesses. Table IV indicates the different types of organizations. The participants represented 33 governmental organizations and 25 private organizations. These were the two largest categories. The third and fourth largest categories were higher education (15 participants) and military (13 participants), with one percentage point separating the two groups.

TABLE IV. Organization Breakdown

Which one describes your organization?	Number of Participants	% of Participants
Governmental	33	30%
Local State	3	3%
Private	23	23%
Non-Profit	10	9%
Military	13	13%
Higher Education	15	14%
K12	3	3%
Other	5	5%

Professors appear to have different methods of teaching styles based on their status. Table V shows the classification of participating professors. Twenty-seven full-time faculty members, eight part-time faculty members, and 10 adjunct faculty members completed the survey. There is a difference between part-time faculty members and adjunct faculty members because part-time faculty members can teach more

than two courses in any term, while adjunct faculty cannot. All of the professors answered the questions based on their levels of education in the field of cybersecurity and depending on their classifications. For example, a full-time professor who has a computer science background would have answered differently from someone with a background in management information systems (MIS) or computer information systems, with a heavy security background. The part-time faculty members and adjunct faculty members may be working in the field of cybersecurity and could have influenced their answers.

TABLE V. PROFESSOR EMPLOYMENT BREAKDOWN

Do you consider yourself	**Number of Participants**	**% of Participants**
Full-Time Faculty	27	61%
Part-Time Faculty	7	16%
Adjunct Faculty	10	23%

As Table VI indicates, 70 participants (67%) worked or supervised personnel in the cybersecurity industry. Table VII indicates that 37 participants currently worked or previously worked with a recent cybersecurity graduate. Table VIII indicates that 73% of the 37 participants, who answered "yes" from Table VII, were satisfied with their recent cybersecurity graduates.

TABLE VI. WORKING WITH OTHERS IN THE CYBER SECURITY INDUSTRY

Do you currently work or supervise personnel in the cybersecurity industry?	**Number of Participants**	**% of Participants**
Yes	70	67%
No	35	33%

TABLE VII. WORKING WITH RECENT CYBER SECURITY GRADUATES

Do you currently or have you previously worked with a recent cybersecurity graduate(s)?	**Number of Participants**	**% of Participants**
Yes	37	53%
No	33	47%

TABLE VIII. OVERALL SATISFACTION WITH RECENT CYBER SECURITY GRADUATES

Overall, how satisfied are you with the recent cybersecurity graduate(s)?	**Number of Participants**	**% of Participants**
Very Satisfied	11	30%
Satisfied	16	43%
Neutral	8	22%
Dissatisfied	2	5%
Very Dissatisfied	0	0%

TABLE IX. IMPRESSION OF RECENT GRADUATES BREAKDOWN

What was your impression of the recent graduate(s) you hired or worked with?	**Number of Participants**	**% of Participants**
Positive Comments	22	60%
Negative Comments	10	27%
No Comment	1	3%
Positive and Negative Comments	4	10%

The professionals, who expressed their overall satisfaction with recent cybersecurity graduates, also had the opportunity to answer an open-ended question. This question asked, "What was your impression of recent graduates you hired or worked with?" All 37 participants left their impressions of a recent cybersecurity graduate (See Table IX).

Overall, 73% of the participants indicated satisfaction with recent cybersecurity graduate(s). From an assessment of the qualitative data, a codebook was established to link common themes and patterns. Its purpose was to show patterns and extract themes from the data. Next, phrases/comments were placed in groups based on keywords and reviewed them. Four positive themes appeared: (a) graduates have good knowledge about the field, (b) graduates have a good skill set to meet performance demands, (c) graduates have a willingness to learn, and (d) graduates are technically savvy and open-minded towards mentoring. Two participants elaborated further. According to Participant #37669584, "Almost all of the recent graduates have 'high levels' of security knowledge" and "are skill orientated and willing to learn." Another participant (#43595549) confirmed this by stating recent graduates are "very

competent, clearly well versed in InfoSec procedures and terminology" and they "know how to meticulously break down problems to find the root and applicable solution."

Although 73% of the professionals are happy with recent graduates in the cybersecurity field, the data showed evident disagreement. One common negative theme was a gap or deficiency in university programs. One participant (#45400509) stated the following:

> Cyber is a very broad field and the range of today's cyber grads are even broader. Ones with some job experience do better than those that just have a degree. Personality and initiative count for a lot as in most fields. [There are] deficiencies in making the jump from the academic world to the real world; fitting the recent grads to the right job is critical.

The same group of professionals had the chance to answer another open-ended question. Question 5c on the survey asked participants, "How were they prepared or not prepared for their profession?" Thirty-six of these participants left comments on the preparedness of recent cybersecurity graduates. Overall, 43% of these professionals believed that recent graduates were prepared for their profession (See Table X).

TABLE X. RECENT GRADUATE PREPARATION BREAKDOWN

How were they prepared/not prepared for their profession?	**Number of Participants**	**% of Participants**
Prepared	16	43%
Not Prepared	11	30%
No Comment	1	3%
Prepared and Not Prepared	9	24%

The results highlighted in Table X are very similar to the findings of a 2018 national workforce study, which surveyed 1000 college students, and determined 41% of college students feel very or extremely prepared for their future careers [23]. In other words, the professionals' expectations mirror the students' own anticipations.

Five common themes emerged from the word frequencies and patterns in the data. However, an additional negative theme emerged, suggesting a need for mentoring and offering hands-on experience, such as internships, before cybersecurity students' graduation. The five central themes cast a positive light on the recent graduates: (a) graduates understand the nature of security and instructions; (b) graduates have a strong working knowledge of security systems and protocols and software; (c) graduates understand the nature of the business of security; (e) graduates understand the nature of security critical thinking, and evaluation skill sets; and (f) graduates are willing to learn and grow skill sets in the field. Student participants provided several insights concerning cybersecurity competencies. One participant explained:

> The ability to investigate issues, warnings, and errors in logs; the knowledge of basic operations of network devices [so] as to enable them to spot anomalies; be motivated to take the initiative in creating policies, educating users, researching issues and staying well informed on current trends is a core competency in the field.

Other participants remarked about a positive learning approach, fundamental skill set mastery, basic cybersecurity mastery, and ability to adapt independently. The most common theme was the graduates' abilities to communicate with the stakeholder. Another participant (#453430934) noted that the students can "communicate aforementioned competencies to a client with no technical expertise, in a clear manner, so he or she knows where or when [to] be concerned about security issues."

V. FUTURE RESEARCH

This project builds a solid foundation for additional and complementary research. Through this pioneering research, we now know that the majority (73%) of the cybersecurity professionals are satisfied with recent cybersecurity graduates. The project also determined that most (67%) of the respondent professionals believed that recent graduates had a satisfactory level of competency. Equally, it is interesting to note the level of the professionals reported level of graduates' preparedness (43%) is very similar to that reported by students (41%).

The next step should be to examine the characteristics and skills that enhance the satisfaction of cybersecurity professionals and the preparedness of graduates. Specifically, future research should address to the knowledge and keys that might increase employer satisfaction and student preparedness. For example, a recent in report chronicling the wants and needs of employers in North American organizations highlighted five core areas that were rated above 90% in an importance scale (Adaptability, Problem-solving, Teamwork, Communication, and Interpersonal skills) [24]. Interestingly, the same study found a 12-point difference in importance and satisfaction scores reported by employers. Would enhancing these core skills result in a corresponding increase in satisfaction and/or preparedness?

VI. SUMMARY

The explicit aim of the project was to assess supervisors' satisfaction with recent cybersecurity graduates within their organizations. In other words, answer the question, Are cybersecurity professionals satisfied with recent cybersecurity graduates? To achieve this aim, a survey instrument was developed and administered to cybersecurity professionals. A total of 129 participants started the survey, while 105 cybersecurity professionals completed the survey, giving an 81% participation rate.

The sample was 82.9% male participants and 17.1% female participants. In terms of organizational management level, 31% of the participants self-identified as middle management, 18% selected upper-level management, and 11% cited lower-level management. In addition, 39% of the sample choose individual contributor (22% with no hiring influence and 17% with hiring preference). Eighty percent of the respondents were from four broad organizational types: governmental (30%), private (23%), military (13%) and higher education (14%). Sixty-seven percent of the participants worked or supervised personnel in the cybersecurity industry and 53% participants currently worked or previously worked with a recent cybersecurity graduate.

The most important finding of the project was that 73% of the participants indicated satisfaction with recent cybersecurity graduates, thus answering the question, Are cybersecurity professionals satisfied with recent cybersecurity graduates? Just 5% of the participants reported they were dissatisfied. Equally important was the discovery that 43% of these professionals believed that recent graduates prepared for their profession; however, 30% indicated that the graduates were not prepared.

An implicit aim of the project was to be the catalyst for additional research. Very little rigorous research has been published in the nascent domain of cybersecurity, especially in the subdomains of cybersecurity graduate competency and employer satisfaction. This project has created a solid foundation upon which other projects may build.

REFERENCES

[1] P. E. Ceruzzi, A History of Modern Computing, London: MIT Press, 2003.

[2] H. F. Tipton and M. Krause, "Managing Security Issues," *Information Security Management Handbook, Sixth Edition, Volume 1*, pp. 12-12, 2008.

[3] L. Winmill, D. Metcalf and M. Band, "CYBERCRIME: ISSUES AND CHALLENGES IN THE UNITED STATES," *Digital Evidence & Electronic Signature Law Review*, pp. 719-34, 2010.

[4] "Federal Computer Systems Protection Act," 27 June 1977. [Online]. Available: https://www.congress.gov/bill/95th-congress/senate-bill/1766.

[5] "HomeDepot," 6 Nov 2014. [Online]. Available: https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf.

[6] Microsoft, "Safety & Security Center," 2014. [Online]. Available: https://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx.

[7] "Office of HIPAA Privacy & Security," 2015. [Online]. Available: http://privacyoffice.med.miami.edu/faq/privacy-faqs/what-is-personally-identifiable-information-pii.

[8] D. O. McGee, "Tech expert discusses cyberattacks' far-reaching consequences," 06 Feb 2014. [Online]. Available: http://gsnmagazine.com/article/40152/tech_expert_discusses_cyberattacks%E2%80%99_far_reaching_c.

[9] B. Obama, "Remarks by the President in State of the Union Address | January 20, 2015," 20 Jan 2015. [Online]. Available: https://www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015.

[10] L. C. Baldor and P. Jelinek, "Pentagon plans to triple cybersecurity staff," 28 Mar 2014. [Online]. Available: http://www.pbs.org/newshour/rundown/pentagon-plans-triple-cybersecurity-staff/.

[11] K. Carapezza, "With more than 200,000 unfilled jobs, colleges push cybersecurity.," 22 Jan 2015. [Online]. Available: http://www.pbs.org/newshour/updates/college-struggle-keep-pace-need-cyber-soliders/.

[12] D. Lawrence, "The U.S. Government Wants 6,000 New 'Cyberwarriors' by 2016," 15 April 2014. [Online]. Available: http://www.businessweek.com/articles/2014-04-15/uncle-sam-wants-cyber-warriors-but-can-he-compete.

[13] "Occupational Outlook Handbook," 8 Jan 2014. [Online]. Available: http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

[14] "Educate to Innovate," April 2013. [Online]. Available: https://www.whitehouse.gov/issues/education/k-12/educate-innovate.

[15] NICE, "Curriculum Resources: Teaching Tools for Educators," 20 February 2015. [Online]. Available: http://niccs.us-cert.gov/education/curriculum-resources.

[16] P. Rubens, "018 IT Security Employment Outlook: Which Security Skills and Certs are Hottest?," Security Planet, 2017. [Online]. Available: https://www.esecurityplanet.com/network-security/2018-it-security-employment-outlook.html.

[17] A. Rayome, "The 5 most in-demand cybersecurity roles in the age of GDPR," Tech Repiblic, 2018. [Online]. Available: https://www.techrepublic.com/article/the-5-most-in-demand-cybersecurity-roles-in-the-age-of-gdpr/.

[18] S. Ivancevich, D. Ivancevich and R. Roscher, "The First Two Years of Employment," *CPA Journal*, vol. 79, no. 7, pp. 69-72, 2009.

[19] D. F. Treadwell and J. B. Treadwell, "Employer Expectations of Newly-Hired Communication Graduates," *Journal Of The Association For Communication Administration 28, no. 2*, pp. 87-99, 1999.

[20] M. H. Kavanagh and L. Drennan, "What skills and attributes does an accounting graduate need? Evidence from student perceptions and employer expectations," *Accounting & Finance, 48(2)*, pp. 279-300, 2007.

[21] P. Nardi, Doing Survey Research: A guide to quantitative Methods, Boulder: Paradigm, 2014.

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

[23] McGraw-Hill, "2018 McGraw-Hill Future Workforce Survey," McGraw-Hill Education, New York, 2018.

[24] Institute of Student Employers, "The Global Skills Gap in the 21st Century," QS, London, 2018.