# Judging Competencies in 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 innovative research project chronicles how cybersecurity professionals and professors rate recent cybersecurity graduates in the components of Cybersecurity Competency Model. Noteworthy findings included that information technology graduates exhibit poor reading, writing, and some communication skills; there was a statistically significant difference between the two groups in their thoughts on the importance of mathematics; and there was a significant difference between the two groups pertaining to (a) planning and organization and (b) working with tools of technology.**

***Keywords—cybersecurity, graduates, competencies, expectations***

## I. Introduction

The National Cybersecurity Workforce Framework proposed to connect colleges, training vendors, students, employers, employees, and policymakers to align degrees, job training, and certifications for cybersecurity. It also developed a "comprehensive competency model for cybersecurity" [1, p. 1] by using subject matter expert from the workforce and academic. The Cybersecurity Competency Model defines "the latest skills and knowledge requirements needed by individuals whose activities impact the security of their organization's cyberspace" [1, p. 1].

The Cybersecurity Industry Model (CIM) was designed to provide a framework to help employers decide on which competencies are needed by a cybersecurity professional from an entry-level employee to management. The person designated as a cybersecurity professional will help to secure a company's network from both internal and external threats [1]. CIM defines cybersecurity or cyberspace, for the purpose of the model, as the following: "The strategy, policy, and standards regarding the security of and operations in cyberspace, whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation" [1, p. 3].

The Cybersecurity Competency Model (CSCM) was released by The Employment and Training Administration (ETA). The overall aim of this study was to identify 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. A prior report considered Tier 1 [2] while another report focused specifically on whether cybersecurity professionals satisfied with recent cybersecurity graduates [3]. This part of the project considered how cybersecurity professionals and cybersecurity profession rate the importance of CSCM tiers 2 through 5.

Tier 2 contains the academic skills level. This is where an employer rates a potential employee's ability to learn common core education. The employer can use this level to rule out any person without a certain Grade Point Average (GPA) or lack in a common core area. Employers may like to see if this potential employee had a previous internship. An internship would greatly enhance a person's abilities in the next three levels of Tiers. The competencies at this level are the following: reading, writing, mathematics, science, communication, critical and analytic thinking, and fundamental IT skills. For Tier 2, "Academic Competencies are primarily learned in a school setting. They include cognitive functions and thinking styles. Academic competencies are likely to apply to all industries and occupations" [3, p. 10].

Tier 3 is the working environment skills level. This is where an employer can separate a recent college graduate from someone who has been in the profession for a number of years. Most of these skills can be learned in different ways. For a recent college graduate, several of the skills can be learned through academic coursework, college-sponsored clubs, organizations, and at home. There are numerous different ways someone could learn all the different skills, but ultimately the potential employee would need to show competency in the work environment for which they are applying. The competencies for this level are the following: teamwork, planning and organizing, critical thinking, problem-solving and decision making, working with tools and technology, and business fundamentals. For Tier 3, "Workplace Competencies represent motives and traits, as well as interpersonal and self-management styles. These are generally applicable to a large number of occupations and industries" [3, p. 17].

Tier 4 is the industry standard skills level, and again at this level, the employer can separate a recent graduate from

a professional. Basic skills can be taught in the classroom but, to be proficient at this level, one must have on the job experience for a certain amount of time. This experience gives employees time to learn the business and how to react in real-world situations. Employers expect potential employees to understand and execute five main functions as it relates to the company's mission. The competencies at this level are the following: cybersecurity technology, information assurance, risk management, incident detection, and incident response and remediation [3].

Tier 5 is industry sector skills level. At this level, employers can create and define an employee's role within the company. Because these skills are specialized functions, a potential employee could have one or two areas in this skill set, as their main responsibilities for day-to-day operations. This could depend on the size of the company or special needs of each company. Some of these skills can be learned within the classroom, but to understand the job or task, a particular employer needs an employee to work in the position and perform the duties. The competencies at this level include security provision systems, operate and maintain IT security, protect and defend from threats, investigate threats, collect information and operate cybersecurity process, analyze information, and oversee and govern cybersecurity work.

## II. Methodology

Two surveys were used to collect the necessary data. The first survey was administered to 104 cybersecurity professionals and second survey was administered to 44 cybersecurity professors. Both surveys were designed to take no more than 10–15 minutes of the participants' time, with no more than 15 questions, depending on the participants' answers. The small number of survey questions helped to ensure that participants did not reach survey fatigue.

The criteria for group one (Professional) included (a) cybersecurity professional and (b) currently or previously employed or supervised someone in the cybersecurity industry. The rationale for this criteria selection was to gather input from employers because the best results required engaging cybersecurity professionals or supervisors already in the field. The criteria for group two (Professor) included (a) a faculty member and (b) having taught cybersecurity courses at the university level. The rationale for this criteria selection was to involve educators since it was a logical choice to engage educators on how they lecture students and how they develop curriculum.

The first part of both surveys included questions demographic and professional attributes and characteristics. 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. An example, (shown in Figure 1 focused on the Personal Effectiveness Competencies. The question 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" [3, 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 | ❑ | ❑ | ❑ | ❑ | ❑ |

Fig. 1. Personal effectiveness competencies.

Academic Competencies are primarily learned in a school setting. They include cognitive functions and thinking styles. Academic competencies are likely to apply to all industries and occupations.

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

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

| | Very Important | Important | Neutral | Less Important | Not Important |
|---|---|---|---|---|---|
| Reading | ❑ | ❑ | ❑ | ❑ | ❑ |
| Writing | ❑ | ❑ | ❑ | ❑ | ❑ |
| Mathematics | ❑ | ❑ | ❑ | ❑ | ❑ |
| Science and Technology | ❑ | ❑ | ❑ | ❑ | ❑ |
| Communication | ❑ | ❑ | ❑ | ❑ | ❑ |
| Critical and Analytic Thinking | ❑ | ❑ | ❑ | ❑ | ❑ |
| Fundamental IT User Skills | ❑ | ❑ | ❑ | ❑ | ❑ |

Fig. 2. Academic competencies

The next question (shown in Figure 2) focused on the Academic Competencies, "which were characteristics primarily learned in a school setting" (DOL, 2014, p. 10). These competencies included cognitive functions and thinking styles. Academic Competencies "were likely to apply to all industries and occupations" [3, p. 10].

One question (shown in Figure 3) focused on the Workplace Competencies, which were "represented by motives and traits, as well as interpersonal and self-management styles" (DOL, 2014, p. 17). DOL found these characteristics "generally applicable to a large number of occupations and industries" [3, p. 17].

Workplace Competencies represent motives and traits, as well as interpersonal and self-management styles. They are generally applicable to a large number of occupations and industries.

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

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

| | Very Important | Important | Neutral | Less Important | Not Important |
|---|---|---|---|---|---|
| Teamwork | ❑ | ❑ | ❑ | ❑ | ❑ |
| Planning and Organizing | ❑ | ❑ | ❑ | ❑ | ❑ |
| Creative Thinking | ❑ | ❑ | ❑ | ❑ | ❑ |
| Problem Solving and Decision-Making | ❑ | ❑ | ❑ | ❑ | ❑ |
| Working with Tools and Technology | ❑ | ❑ | ❑ | ❑ | ❑ |
| Business Fundamentals | ❑ | ❑ | ❑ | ❑ | ❑ |

Fig. 3. Workplace competencies.

Industry-Wide Technical Competencies cover the knowledge, skills, and abilities from which workers across the industry can benefit, regardless of the sector in which they operate. These competencies are considered cross-cutting, as they allow a worker to move easily across industry subsectors. Because of this, many of the critical work functions on this tier deal with awareness or understanding, rather than performing specific job tasks.

Professional: How important are Industry-Wide Technical Competencies when hiring or working with recent cyber security graduates?

Professor: How important do you think it is to incorporate the following Industry-Wide Technical Competencies into the curriculum when teaching cyber security courses?

| | Very Important | Important | Neutral | Less Important | Not Important |
|---|---|---|---|---|---|
| Cyber-security Technology | ❑ | ❑ | ❑ | ❑ | ❑ |
| Information Assurance | ❑ | ❑ | ❑ | ❑ | ❑ |
| Risk Management | ❑ | ❑ | ❑ | ❑ | ❑ |
| Incident Detection | ❑ | ❑ | ❑ | ❑ | ❑ |
| Incident Response and Remediation | ❑ | ❑ | ❑ | ❑ | ❑ |

Fig. 4. Industry-wide technical competencies

The next question (shown in Figure 4) focused on Industry-Wide Technical Competencies. This question covered the following:

*Knowledge, skills, and abilities from which workers across the industry benefited, regardless of the sector in which they operated. These competencies were considered crosscutting, as they allowed a worker to move easily across industry subsectors. Because of this, most of the critical work functions on this tier dealt with awareness or understanding, rather than performing specific job tasks. [3, p. 22*

The penultimate question (shown in Figure 5) focused on Industry-Sector Functional Areas. This "established the common taxonomy and lexicon that was to be used to describe all cybersecurity work and workers irrespective of where or for whom the work was performed" [3, p. 40]. The last question of this survey was open-ended, see Figure 6. The purpose of this question was to capture any ideas, thoughts, or responses that were not available to the participants in the previous questions [4].

Industry-Sector Functional Areas establish the common taxonomy and lexicon that is to be used to describe all cybersecurity work and workers irrespective of where or for whom the work is performed.

Professional: How important are Industry-Sector Functional Areas when hiring or working with recent cyber security graduates?

Professor: How important do you think it is to incorporate the following Industry-Wide Technical Competencies into the curriculum when teaching cyber security courses?

| | Very Important | Important | Neutral | Less Important | Not Important |
|---|---|---|---|---|---|
| Securely Provision Systems | ❑ | ❑ | ❑ | ❑ | ❑ |
| Operate and Maintain IT Security | ❑ | ❑ | ❑ | ❑ | ❑ |
| Protect and Defend from Threats | ❑ | ❑ | ❑ | ❑ | ❑ |
| Investigate Threats | ❑ | ❑ | ❑ | ❑ | ❑ |
| Collect Information and Operate Cybersecurity Processes | ❑ | ❑ | ❑ | ❑ | ❑ |
| Analyze Information | ❑ | ❑ | ❑ | ❑ | ❑ |
| Oversee and Govern Cybersecurity Work | ❑ | ❑ | ❑ | ❑ | ❑ |

Fig. 5. Industry-sector functional areas.

**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?

Fig. 6. Open-ended question

## III. RESULTS

Cybersecurity professionals and professors from across the United States completed separate, independent surveys. The results are separated into two categories: Professionals (Pro) and Professors (Prof), with a total of 105 cybersecurity professionals and 44 cybersecurity professors who participated in this research. The overall results on academic competencies are in Table I and Table II.

TABLE I. PROFESSIONAL: ACADEMIC COMPETENCIES BREAKDOWN

| Pro – Academic Competencies | Very Important | | Important | | Neutral | | Less Important | | Not Important | |
|---|---|---|---|---|---|---|---|---|---|---|
| | % | N | % | N | % | N | % | N | % | N |
| Reading | 50% | 53 | 43% | 45 | 6% | 6 | 1% | 1 | | |
| Writing | 50% | 53 | 42% | 44 | 7% | 7 | 1% | 1 | | |
| Mathematics | 20% | 21 | 46% | 48 | 28% | 29 | 6% | 6 | 1% | 1 |
| Science and Technology | 43% | 45 | 47% | 49 | 8% | 9 | 2% | 2 | | |
| Communication | 64% | 67 | 33% | 35 | 2% | 2 | 1% | 1 | | |
| Critical and Analytic Thinking | 87% | 92 | 10% | 10 | 3% | 3 | | | | |
| Fundamental IT User Skills | 63% | 66 | 31% | 33 | 4% | 4 | 2% | 2 | | |

TABLE II. PROFESSOR: ACADEMIC COMPETENCIES BREAKDOWN

| Prof – Academic Competencies | Very Important | | Important | | Neutral | | Less Important | | Not Important | |
|---|---|---|---|---|---|---|---|---|---|---|
| | % | N | % | N | % | N | % | N | % | N |
| Reading | 79% | 35 | 16% | 7 | 5% | 2 | | | | |
| Writing | 68% | 30 | 27% | 12 | 5% | 2 | | | | |
| Mathematics | 39% | 17 | 43% | 19 | 14% | 6 | 2% | 1 | 2% | 1 |
| Science and Technology | 66% | 29 | 27% | 12 | 5% | 2 | | | 2% | 1 |
| Communication | 82% | 36 | 16% | 7 | 2% | 1 | | | | |
| Critical and Analytic Thinking | 93% | 41 | 5% | 2 | 2% | 1 | | | | |
| Fundamental IT User Skills | 68% | 30 | 27% | 12 | 2.5% | 1 | 2.5% | 1 | | |

A two-tailed *t* test was used to examine the relationship between professional and professor responses. This test is used to compare if any differences exist between two different groups. A probability of less than .05 would show a statistically significant difference between the two groups. As Table III shows, the *t* test results for academic competencies, between the two groups, revealed statistically significant differences with regard to reading ($t = -3.14$, $df = 97.24$, $p < .002$); writing ($t = -2.01$, $df = 92.36$, $p < .047$); mathematics ($t = -2.21$ $df = 77.63$, $p < .030$); and communication ($t = -2.17$, $df = 100.84$, $p < .032$).

TABLE III. ACADEMIC COMPETENCIES FOR PROFESSIONALS AND PROFESSORS

| ***t* Test Result – Academic Competencies** | ***p*** | **Result** |
|---|---|---|
| Reading | .002 | The result is significant at p < .05 |
| Writing | .047 | The result is significant at p < .05 |
| Mathematics | .030 | The result is significant at p < .05 |
| Science and Technology | .085 | The result is not significant at p < .05 |

| ***t* Test Result – Academic Competencies** | ***p*** | **Result** |
|---|---|---|
| Communication | .032 | The result is significant at p < .05 |
| Critical and Analytic Thinking | .376 | The result is not significant at p < .05 |
| Fundamental IT User Skills | .600 | The result is not significant at p < .05 |

A frequency analysis revealed a significant difference in that 79% of the professors agreed with 50% of the professionals that reading is very important. A significant difference existed ($p < .002$), as 42% of the professionals chose reading as important, and only 16% of the professors agreed with them (see Table I and Table II). The significant difference, as related to the reading competency, is that professors may read more than an average person and they understand the value of reading while cybersecurity professionals tend to read the technical manuals relating to the field. A study conducted by Treadwell and Treadwell [5] found that employers were dissatisfied with the academic performance from recent graduates.

Another frequency analysis showed that 68% of the professors agreed with 50% of the professionals that writing is very important. A significant difference existed ($p < .047$), as 42% of the professionals chose writing as important, and only 27% of the professors agreed with them (see Table I and Table II). Professors and professionals both agree that the writing competency is very important or important in the workforce. The significant difference in the writing competency depends on a person's job duties, which varies from position to position. Treadwell and Treadwell's found employers were not impressed when they received cover letters and resumes that had basic grammar errors and they were neutral about "Dear first name" in a cover letter when there is a relationship between the parties. [5, p. 91]

A frequency analysis showed that 64% of the professors agreed with 82% of the professionals that communication is very important. A significant difference existed ($p < .032$) between professionals (33%), who chose communication as important and only 16% of the professors (see Table I and Table II). These findings are consistent with Treadwell and Treadwell's [5] conclusion that recent graduates are not completely ready for the workforce.

The overall results for workplace competencies are in Table IV and Table V.

TABLE IV. PROFESSIONAL: WORKPLACE COMPETENCIES BREAKDOWN

| **Pro – Workplace Competencies** | **Very Important** | | **Important** | | **Neutral** | | **Less Important** | | **Not Important** | |
|---|---|---|---|---|---|---|---|---|---|---|
| | % | N | % | N | % | N | % | N | % | N |
| Teamwork | 51% | 54 | 45% | 47 | 3% | 3 | 1% | 1 | | |
| Planning and Organizing | 39% | 41 | 50% | 53 | 8% | 8 | 3% | 3 | | |
| Creative Thinking | 50% | 53 | 42% | 44 | 4% | 4 | 4% | 4 | | |
| Problem Solving and Decision-Making | 73% | 77 | 27% | 28 | | | | | | |
| Working with Tools and Technology | 50% | 53 | 40% | 42 | 8% | 8 | 1% | 1 | 1% | 1 |
| Business Fundamentals | 26% | 27 | 39% | 41 | 29% | 30 | 5% | 6 | 1% | 1 |

TABLE V. PROFESSOR: WORKPLACE COMPETENCIES BREAKDOWN

| **Prof – Workplace Competencies** | **Very Important** | | **Important** | | **Neutral** | | **Less Important** | | **Not Important** | |
|---|---|---|---|---|---|---|---|---|---|---|
| | % | N | % | N | % | N | % | N | % | N |
| Teamwork | 61% | 27 | 27% | 12 | 8% | 3 | 2% | 1 | 2% | 1 |
| Planning and Organizing | 59% | 26 | 36% | 16 | 5% | 2 | | | | |
| Creative Thinking | 61% | 27 | 34% | 15 | 5% | 2 | | | | |
| Problem Solving and Decision-Making | 84% | 37 | 14% | 6 | 2% | 1 | | | | |
| Working with Tools and Technology | 70% | 31 | 23% | 10 | 7% | 3 | | | | |
| Business Fundamentals | 27% | 12 | 53% | 23 | 11% | 5 | 9% | 4 | | |

To determine the relationship between professionals and professors, a two-tailed *t* test was used to determine if a difference existed. Table VI shows the *t* test results for workplace competencies. There were statistically significant differences between the two groups regarding planning and organizing ($t = -2.55$, $df = 98$, $p < .012$) and working with tools and technology ($t = -2.164$, $df = 98.08$, $p < .033$).

TABLE VI. WORKPLACE COMPETENCIES FOR PROFESSIONALS AND PROFESSORS

| ***t* Test Result – Workplace Competencies** | ***p*** | **Result** |
|---|---|---|
| Teamwork | .815 | The result is not significant at p < .05 |
| Planning and Organizing | .012 | The result is significant at p < .05 |
| Creative Thinking | .123 | The result is not significant at p < .05 |
| Problem Solving and Decision-Making | .292 | The result is not significant at p < .05 |
| Working with Tools and Technology | .033 | The result is significant at p < .05 |
| Business Fundamentals | .353 | The result is not significant at p < .05 |

A frequency analysis showed that 59% of the professors agreed with 39% of the professionals that planning and organizing is very important. A further significant difference existed, as 50% of the professionals chose planning and organizing as important, and only 36% of the professors agreed with them (See Table IV and Table V). A possible difference between the two groups is that professors can teach planning and organizing in a clean, static environment while professionals plan and organize in chaotic, dynamic environments. Ivancevich et al. [6] echoed this and added the importance of teamwork, time management, and understanding the needs of the clients to accomplish a given task.

A frequency analysis, of "very important" responses to the tools and technical competency, showed 70% of professors agreed while 50% of professionals agreed. Of the "important" responses, a difference, ($p < .033$) between 40% of the professionals chose to work with tools and technology as important, and only 23% of the professors agreed with them (See Table IV and Table V). There is a significant amount of software/hardware tools and technology available for any company to use to defend their network and protect their data. Higher education institutions cannot anticipate which tools and technology will be used in the workforce to help prepare cybersecurity students. These findings agree with Treadwell and Treadwell's [5] and Ivancevich et al. [6] conclusions that recent graduates are not fully ready for the workforce, which also assisted with answer research questions one and two.

The overall results on industry-wide technical competencies are in Table VII and Table VIII.

TABLE VII. PROFESSIONAL: INDUSTRY-WIDE TECHNICAL COMPETENCIES BREAKDOWN

| **Pro – Professional Industry-Wide Technical Competencies** | **Very Important** | | **Important** | | **Neutral** | | **Less Important** | | **Not Important** | |
|---|---|---|---|---|---|---|---|---|---|---|
| | % | N | % | N | % | N | % | N | % | N |
| Cybersecurity Technology | 62% | 66 | 30% | 31 | 7% | 7 | 1% | 1 | | |
| Information Assurance | 54% | 57 | 36% | 38 | 10% | 10 | | | | |
| Risk Management | 50% | 53 | 42% | 44 | 8% | 8 | | | | |
| Incident Detection | 54% | 57 | 37% | 39 | 8% | 8 | 1% | 1 | | |
| Incident Response and Remediation | 56% | 59 | 36% | 38 | 6% | 6 | 1% | 1 | 1% | 1 |

TABLE VIII. PROFESSOR: INDUSTRY-WIDE TECHNICAL COMPETENCIES BREAKDOWN

| **Prof – Professional Industry-Wide Technical Competencies** | **Very Important** | | **Important** | | **Neutral** | | **Less Important** | | **Not Important** | |
|---|---|---|---|---|---|---|---|---|---|---|
| | % | N | % | N | % | N | % | N | % | N |
| Cybersecurity Technology | 75% | 33 | 20% | 9 | 5% | 2 | | | | |
| Information Assurance | 75% | 33 | 23% | 10 | 2% | 1 | | | | |
| Risk Management | 68% | 30 | 30% | 13 | 2% | 1 | | | | |
| Incident Detection | 59% | 26 | 34% | 15 | 7% | 3 | | | | |
| Incident Response and Remediation | 64% | 28 | 32% | 14 | 4% | 2 | | | | |

Table IX shows the *t* test results for industry-wide technical competencies. There were statistically significant differences between the two groups regarding information assurance ($t = -2.814$, $df = 106.32$, $p < .006$) and risk management ($t = -2.293$, $df = 96.45$, $p < .024$).

TABLE IX. INDUSTRY-WIDE TECHNICAL COMPETENCIES

| ***t* Test Result – Industry-Wide Technical Competencies** | ***p*** | **Result** |
|---|---|---|
| Cybersecurity Technology | .129 | The result is not significant at p < .05 |
| Information Assurance | .006 | The result is significant at p < .05 |
| Risk Management | .024 | The result is significant at p < .05 |
| Incident Detection | .518 | The result is not significant at p < .05 |
| Incident Response and Remediation | .241 | The result is not significant at p < .05 |

A frequency analysis showed that 54% of the professors agreed with 75% of the professionals that information assurance is very important. A significant difference exists, as 36% of the professionals chose information assurance as important and only 22% of the professors agreed with them (See Table VII and Table VIII). This competency is important to the business, depending on the type of business and how they view information assurance. Overall, information assurance is a critical area to both groups but distinguishing between those who chose "very important" versus "important" depended upon the respondent's business and the level of management.

Another frequency analysis showed that 50% of the professors agreed with 68% of the professionals that risk management is very important. A statistically significant difference existed ($p < .006$), as 42% of the professionals chose risk management as important and only 30% of the professors agreed with them (see Table VII and Table VIII). Overall, professors and professionals view risk management as an important competency for a cybersecurity graduate. These findings agree with the researchers who developed the CSCM [7].

The responses to industry-sector functional competencies are in Table X and Table XI, with the results in Table XII. The *t* test showed that there were no statistically significant differences between the groups. The Industry-Sector Functional Areas breakdown show that both groups agree on the Industry-Sector Functional Areas Breakdown levels. These competencies are a combination of various skills and attributes to the workforce, which are spread across the first five levels of the model.

TABLE X. PROFESSIONAL: INDUSTRY-SECTOR FUNCTIONAL AREAS BREAKDOWN

| **Pro – Industry-Sector Functional Areas** | **Very Important** | | **Important** | | **Neutral** | | **Less Important** | | **Not Important** |
|---|---|---|---|---|---|---|---|---|---|
| | | N | | N | | N | | N | |
| Securely Provision Systems | 46% | 48 | 41% | 43 | 10% | 11 | 3% | 3 | |
| Operate and Maintain IT Security | 52% | 55 | 42% | 44 | 3% | 3 | 3% | 3 | |
| Protect and Defend from Threats | 66% | 69 | 30% | 32 | 3% | 3 | 1% | 1 | |
| Investigate Threats | 54% | 57 | 31% | 33 | 13% | 13 | 2% | 2 | |
| Collect Information and Operate Cybersecurity Processes | 43% | 45 | 44% | 46 | 10% | 11 | 3% | 3 | |
| Analyze Information | 56% | 59 | 40% | 42 | 2% | 2 | 2% | 2 | |
| Oversee and Govern Cybersecurity Work | 24% | 25 | 50% | 53 | 17% | 18 | 9% | 9 | |

TABLE XI. PROFESSOR: INDUSTRY-SECTOR FUNCTIONAL AREAS BREAKDOWN

| **Prof – Industry-Sector Functional Areas** | **Very Important** | | **Important** | | **Neutral** | | **Less Important** | | **Not Important** | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | N | | N | | N | | N | | |
| Securely Provision Systems | 48% | 21 | 41% | 18 | 11% | 5 | | | | |
| Operate and Maintain IT Security | 61% | 27 | 39% | 17 | | | | | | |
| Protect and Defend from Threats | 70% | 31 | 23% | 10 | 5% | 2 | | | 2% | 1 |
| Investigate Threats | 64% | 28 | 27% | 12 | 7% | 3 | 2% | 1 | | |
| Collect Information and Operate Cybersecurity Processes | 52% | 23 | 34% | 15 | 14% | 6 | | | | |
| Analyze Information | 61% | 27 | 34% | 15 | 5% | 2 | | | | |
| Oversee and Govern Cybersecurity Work | 37% | 16 | 41% | 18 | 20% | 9 | 2% | 1 | | |

TABLE XII. INDUSTRY-SECTOR FUNCTIONAL AREAS FOR PROFESSIONALS AND PROFESSORS

| ***t* Test Result – Industry-Sector Functional Areas** | ***p*** | **Result** |
|---|---|---|
| Securely Provision Systems | .594 | The result is not significant at p < .05 |
| Operate and Maintain IT Security | .083 | The result is not significant at p < .05 |
| Protect and Defend from Threats | .888 | The result is not significant at p < .05 |
| Investigate Threats | .292 | The result is not significant at p < .05 |
| Collect Information and Operate Cybersecurity Processes | .367 | The result is not significant at p < .05 |
| Analyze Information | .559 | The result is not significant at p < .05 |
| Oversee and Govern Cybersecurity Work | .146 | The result is not significant at p < .05 |

## IV. SUMMARY

This study showed that some graduates exhibit poor reading, writing, and some communication skills. Other studies, on the academic disparities between employers and recent graduates, support this conclusion. In these studies, other disciplines face some of the same issues as information technology. For example, students tend to write and speak English that is heavily influenced by slang. Some students thought that was appropriate to write and speak using slang and cryptic acronyms when they communicate with their professors. This aligns with the study of Treadwell and Treadwell [5], who showed that recent graduates lack the proper verbal and written communication skills.

This study highlighted the importance of workplace competencies. There was a significant difference between the two groups pertaining to (a) planning and organization and (b) working with tools of technology. Clearly, organizations differ as such, plan and organize according to their own missions, visions, and ideologies. To improve tools and technology education at academic institutions, universities need to address more than the technologies themselves and the rapid nature at which technologies are fielded. They must consider usability. The field of usability is equally a soft skill, highlighting the phenomena that all cybersecurity competencies are interrelated. There is a need to adequately address and bridge the differing points of view regarding the tools of technology in academia, a recommendation should be presented to higher education institutions to be proactive by constantly informing and advising students to understand and expect a difference between the tools and technologies in the classroom and the essential tools and technology skills employers expect. Higher education institutions should also encourage their students to work with different types of technology tools to be more competitive in the technology workforce.

There are differences in attitude, between employers and professors, concerning information assurance and risk management. There are a number of reasons for this. All organizations differ on how they prioritize and manage risk. For example, a company that does not collect personal identifier information (PII) may not have a robust, restrictive policy on their e-mail or telephone conversations. Conversely, a hospital, which handles highly-sensitive personal health and financial information, is required to safeguard and protect that information by law. These institutions must make risk management a high priority to address and mitigate all vulnerabilities. To address these deficiencies, companies must make a significant investment to train new cybersecurity personnel about IT policies and procedures.

Considering the limited reach and scope of this study, it would be important in the future to increase the size and scope of the dynamic data collection in universities and professionalism. Because of the short time duration of this study, its limited scope, and assessable survey participants, there is a need for greater knowledge before more dynamic generalizations can be considered. The preliminary findings of this study provide useful information for making recommendations to institutions, colleges, and universities of similar size. To generalize these findings, future studies should compare the results of this study with larger universities with greater dynamic influence in career centers, grants, and external funding. This will help develop an understanding of whether there are significant differences because of monetary constraints in budgeting, state funding, or grants.

## REFERENCES

[1] "Cybersecurity Competency Model," 4 January 2015. [Online]. Available: http://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx.

[2] N. St. Clair and J. Girard, "Personal Effectiveness Competencies of Recent Cybersecurity Graduates," *Issues in Information Systems*, to be published.

[3] N. St. Clair and J. Girard, "Employer Perceptions of Recent Cybersecurity Graduates," *The Journal of CISSE, vol. 7, no. 1*, to be published.

[4] DOL, "Cybersecurity Competency Model," 2014. [Online]. Available: http://www.careeronestop.org/CompetencyModel/competency-models/cybersecurity.aspx.

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

[6] 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.

[7] S. Ivancevich, D. Ivancevich and R. Roscher, "The First Two Years of Employment," *CPA Journal, 79(7)*, pp. 69-72, 2009.

[8] "Bureau of Labor Statistics, U.S. Department of Labor," 25 January 2015. [Online]. Available: http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6.

[9] "Curricula Recommendations," 1 Nov 2015. [Online]. Available: http://www.acm.org/education/curricula-recommendations.

[10] 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.