Paper of the Year

Industry Priorities for Cybersecurity Competencies

Michael E. Whitman
mwhitman@kennesaw.edu

Kennesaw State University
560 Parliament Garden Way, MD 0405
Kennesaw, GA 30144

Abstract - With the projected global shortfall of almost 2 million Cybersecurity professionals, it become increasingly critical to promote the development of new Cybersecurity degree programs across the U.S. This raises the question of exactly what should these degree programs prepare students to do? In order to examine this question, this study seeks to identify industry priorities for Cybersecurity competencies based on the Department of Labor's Cybersecurity Industry Model, which creates a tiered set of competencies focusing on the NIST NICE Cybersecurity Workforce Framework categories. The study also seeks to determine if these priorities vary by organizational size or industry.

Keywords

Cybersecurity model, Cybersecurity workforce, Information Security education, Cybersecurity Education

1 INTRODUCTION

The need for future security professionals fills the headlines of computing and industry publications across the globe. The projected massive shortfall of cybersecurity workers over the upcoming decade [1] is viewed as barely stemmed by the expected availability of graduates (Cite) and projected growth as a field [2, 3].

A question which seems to evade those discussing the need for security professionals is exactly what type of security professional is needed. While the expected answer is "all types," it is the specification of these types and their underlying academic preparation which is of most interest to academics responsible for the design and delivery of educational programs.

Some institutions attempt to meet this need by adding security content to existing courses (e.g. [4, 5]), while others add new courses, and still others add entire degree programs. The only constant is the lack of consistency.

One point seems to fall through the gaps when discussing the need for future cybersecurity employees, is that a large number of employees with a wide variety of skills will be needed to perform the 928 tasks, 614 knowledge areas, 359 Skills and 119 Abilities associated with the 172 sample job titles described in the National Institute for Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF; [6]).

1.1 Cybersecurity Education

According to Wilson and Hash (2003), security education "should be focused on developing people's ability and vision to perform complex multi-disciplinary activities and the skills needed to further the cybersecurity profession and to keep pace with threats and technology changes." In 2010, the National Institute for Standards and Technology (NIST) established the National Initiative for Cybersecurity Education (NICE; See csrc.nist.gov/nice/about/). NICE in turn

developed the Cybersecurity Workforce Framework as an effort to define, classify and eventually standardize the terminology associated the numerous security-related positions in the federal government. The result was a set of 31 specialty areas each of which correspond to a field of work in Cybersecurity, organized into seven domains or categories. The framework also includes detailed knowledge, skills and abilities associated with these specialty areas. The NICE Framework was further extended by the Department of Labor's Cybersecurity Industry Model (CIM), as shown in Figure 1.

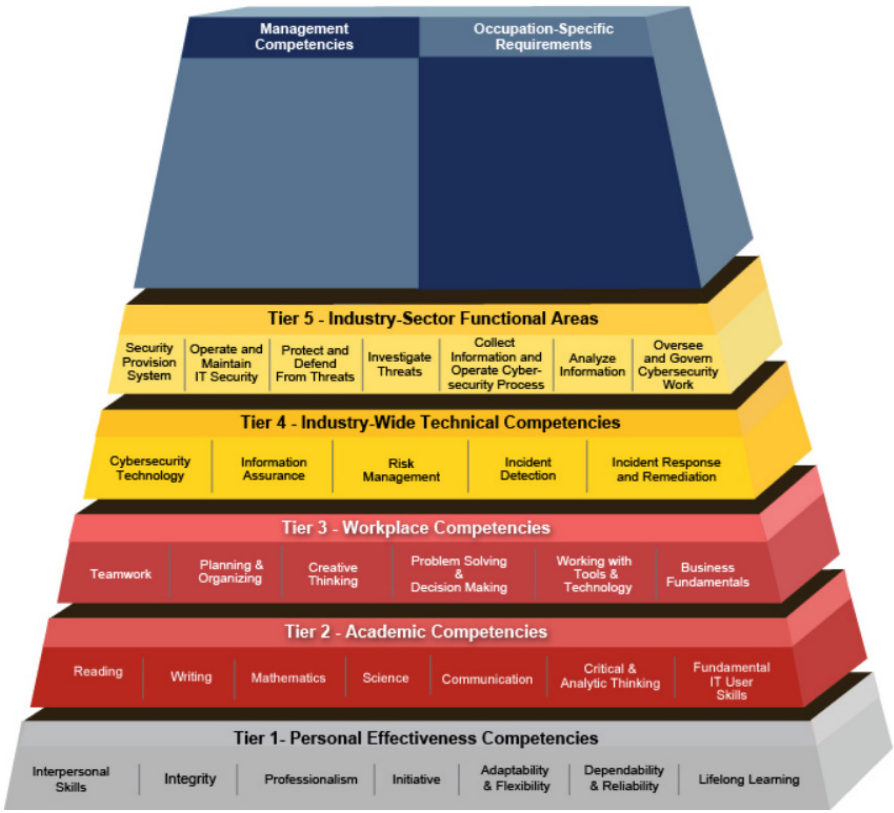

Figure 1: DoL Cybersecurity Industry Model [7]

The purpose of this study is to assess industry priorities and preferences for competencies in entry-level cybersecurity employees, based on the DoL model. As such the following research questions will be examined:

- What are the priority of preferences for entry-level cybersecurity professionals for each of the Tiers of the DoL CIM?
- Do these preferences vary by industry?
- Do these preferences for entry-level cybersecurity professionals vary by organizational size?

2 BACKGROUND

When examining Information Security as a discipline, one finds that there is no simply approach to labeling or defining what an information security curriculum should be. Information security concerns technical information security issues and non-technical (human-related) information security issues [8] but studies have focused largely on technical issues, thus neglecting the non-technical human-related issues as far back as the early 2000's [9, 10, 11, 12, 13]. This is evident in the fact that experts pay more attention to technical issues (such as encryption and firewalls) than to hazards caused by end-users' lack of ISA [8, 14, 15, 16]. Information security has become an issue that no business can disregard; therefore, the non-technical issues should receive the same attention as the technical issues [17, 18].

2.1 Competencies in Cybersecurity Education

The use of the term competencies in this context describes a degree program focused on key fundamental skills or abilities to which a graduate must be capable to demonstrate upon matriculation. In the context of this study, it is not the delivery model, but the underlying academic knowledge that is focused on key competencies. Competency-based curriculum development and assessment is the foundation of most formal curriculum accreditation programs. While ABET incorporates competencies into its accreditation standards, the terms "competency" or "competencies" are not listed explicitly in the Criteria for Accrediting Computing Programs [19]. As one of the newest career fields in business and IT,

Cybersecurity has yet to be formally supported in accreditation standards, although ACM, AIS and IEEE are currently working together through a Joint Task Force to develop standards (see http://www.csec2017.org/), a process which began in 2001 with the ACM IT Education Special Interest Group (SIGITE) [12]. In the initial deliberations of the SIGITE, the committee initially identified eight pervasive "themes":

- "user advocacy
- information assurance and security
- ethics and professional responsibility
- the ability to manage complexity through: abstraction & modeling, best practices, patterns, standards, and the use of appropriate tools
- a deep understanding of information and communication technologies and their associated tools
- adaptability
- life-long learning and professional development
- interpersonal skills" [12].

However, little has been done to determine assessments of these or other related topics as competencies priorities in security education.

Manson, Curl and Torner [20] reported that a survey of academics teaching cybersecurity tend to focus on industry and international standards, such as the CISSP CBK, and the Department of Homeland Security's IT Security Essential body of knowledge as a foundation for security education. Only in recent years has NIST moved to the forefront providing recommendations for content based on the knowledge, skills and abilities of practicing security professionals as the foundation for higher education programs [6]. Figure 2 shows the relatives IA Topic importance from Manson, Curl and Torner's study.

NSTISSI:	Avg.
Security	2.73
Com	2.45
System Ops	2.36
Basics	1.73
AIS Basics	1.64
Planning	1.55
Policies	1.36

CISSP	Avg.
Telecom	2.82
Access	2.55
Apps Sec	2.55
Disaster	2.45
Risk Mgmt	2.36
Ops Sec	2.27
Legal	2.18
Sec Arch	2.18
Env Sec	2.09
Crypto	2.00

DHS	Avg.
Data Security	2.64
Net Secure	2.55
Apps Security	2.40
Incident	2.27
Risk	2.20
Env Secure	2.09
Sys Ops	2.09
Continuity	2.00
Regulatory	2.00
Forensics	1.91
Personnel	1.91
Training	1.91
Strategic	1.90
Procurement	1.27

Figure 2: Importance of IA Topics [20]

According to Wilson and Hash [21], information security education should be focused on "developing people's ability and vision to perform complex multi-disciplinary activities and the skills needed to further the information security profession and to keep pace with threats and technology changes." Sauls and Gudigantala [22] anecdotally recommend that IT security taught to IS majors should "include a solid foundational technical knowledge… understand the IT infrastructures as a system …[and] analytical thinking and problems solving skills."

While earlier studies revealed that older security programs focused heavily on technical security [23], even when the program included non-technical content, it tended to be focused on legal and ethical issues, privacy and other tangentially-related security topics, rather than on managerial security [23, 24]. Studies like Ahmad and Maynard [17] echo the warnings of much earlier studies like Ahmad, Ruighaver and Teo [26] and encouraged the development and promotion of more balanced approaches to meet the breadth of the needs of the information environment.

In spite of the prima fascia recognition of the need for both managerial and technical security topics, a review of these topics reveals insufficient depth and breadth to accurately represent the entire field of security. On a positive note, Soomro, Shah and Ahmed [26], in their comprehensive review of academic literature, find that:

> *"Current research is more concerned with management's role in information security. The trend of considering IT professionals being responsible for information security has changed and now management is believed to be responsible for information security… This study suggests that information security issues should be considered as a responsibility of management, as it has an impact on the market position of a firm" [26].*

2.2 Focus of the Study

This study was specifically designed to assess 1) priorities of industry for the NICE Framework specialty areas appropriate for the private sector–in other words which career fields are in demand in which industries, and 2) priorities of content for competencies of students graduating with a degree in cybersecurity providing information on what the curricular priorities should be in developing and supporting cybersecurity coursework. To the extent possible, these competencies will be examined to determine if differences exist between respondent region, industry and other demographic variables of interest and to examine the relative balance between managerial and technical competencies as desired by organizations in their entry-level employees.

3 METHODOLOGY

The DoL model shown in Figure 1 provided a clear set of competencies by tier, which were converted into a series of questions to determine industry priorities. The initial survey included demographic questions including the respondent's organization's region of operations with the U.S., approximate total number of employees in the organization at all locations, the organization's primary business activity, respondent's job title, and a list of job categories for the respondent to indicate as most closely representative of their job.

For each of the tiers of the DoL Cybersecurity competency model, respondents were asked to rate the competencies from Not Important (=1) to Very Important (=7) for an entry-level cybersecurity employee in their organization. Respondents were then provided with a link to the full definitions of each of the competencies. Each Set of Likert-type responses included a "No Opinion" options in addition to the polar anchored scales.

The resulting online survey was initially reviewed by a panel of experts knowledgeable in research design and cybersecurity education and the NIST NICE framework [6]. Once their recommendations were incorporated, the survey was pilot tested using a database of top security executives and managers in the Atlanta metropolitan area. As part of the pilot project, an open ended question was included at the end of the survey asking for feedback on the survey itself. An email invitation to participate in the survey was emailed to 600 Atlanta-area managers. At the end of the pilot phase, 32 respondents accessed the survey, with 30 completing it, representing a 5% completion rate.

Once the survey was revised based on the pilot study, another invitation to participate was sent out nationwide to the full database of 28,142 top security executives and managers, with bi-weekly reminders. After six weeks, the survey was closed, and resulted in 244 survey attempts. Of the 244 responses, 200 were complete enough to include in the analysis, representing a .71% response rate.

4 FINDINGS

As shown in Figure 3, the largest group of respondents' organizations (23%) were located in Region IV (R4), the Southeast U.S., followed by those organizations identified as operating globally (R-G) at 15%, and those in Region IX (R9) along the Pacific Southwest, islands and territories at 12%.

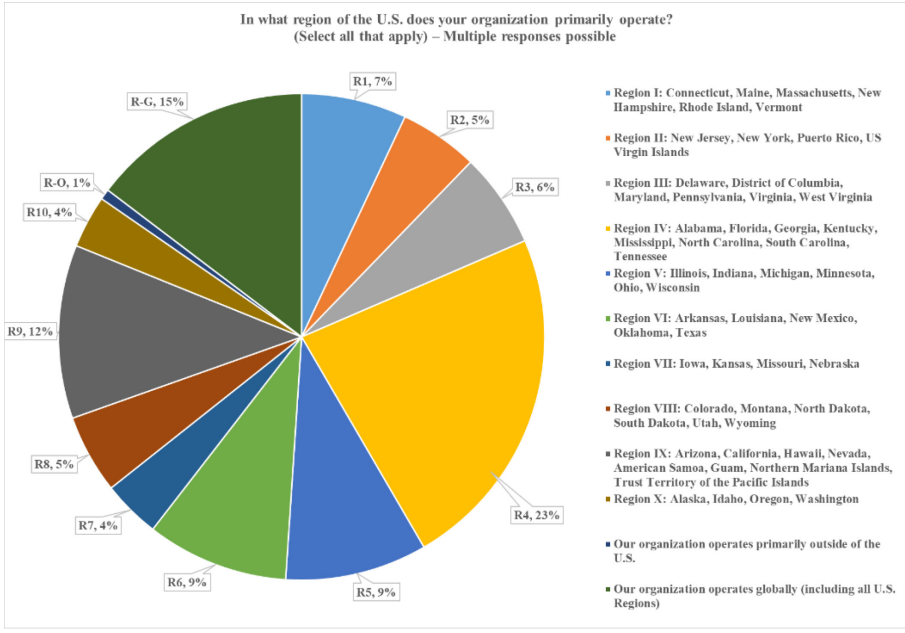

Figure 3: Respondents by Region

Figure 4 illustrates the organization size of respondents. Surprisingly the largest group of respondents at 52% came from extremely large organizations.

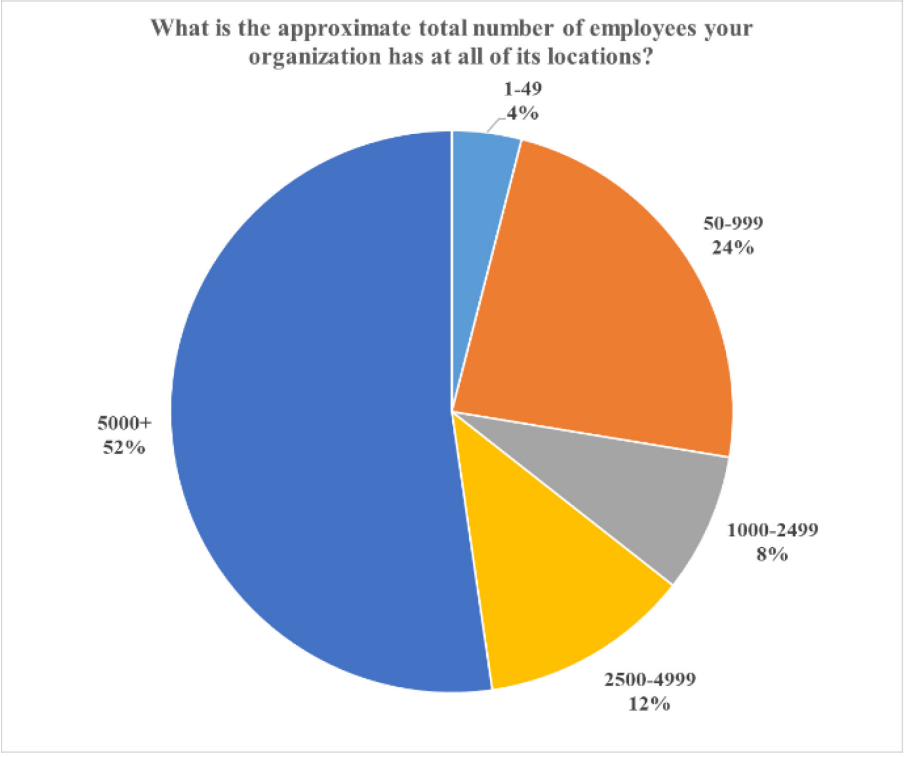

Figure 4: Respondents by Total Number of Employees

Next, as shown in Table 1, respondent's industries were relatively evenly distributed, with the bulk of respondents in Educational Services, Finance/Banking/Insurance/Accounting, Health Care/Social Assistance, and Information Services (Publishing, Communications and Data Processing).

Table 1
Respondents by Industry

What is your organization's primary business activity?	Percent
Agriculture, Forestry, Fishing and Hunting	3.5%
Construction/Architecture/Engineering	1.0%
Educational Services	15.5%
Finance/Banking/Insurance/Accounting	12.5%
Governmental Agencies/Military (exc. Public Services)	9.5%
Health Care/Social Assistance	15.5%
Hospitality (Accommodation and Food Services)	2.0%
Information Services (Publishing, Communications and Data Processing)	15.5%
Manufacturing and Processing (Computer Related)	2.0%
Manufacturing and Processing (exc. Computer Related)	7.5%

Table 1 Respondents by Industry	
What is your organization's primary business activity?	**Percent**
Mining, Quarrying, and Oil and Gas Extraction	.5%
Professional, Scientific, and Technical Services (exc. Construction/Architecture/Engineering)	7.5%
Public Services (exc. Government/Military and Education)	1.0%
Retail/Wholesale Trade	2.0%
Transportation and Warehousing	3.0%
Utilities	1.5%
Other	⋆
Total	100.0

⋆ *The 30 responses originally listed as "Other" provided descriptions of their organization which were then recoded into the original categories by two independent researchers.*

While the job titles of respondents to widely varied to list here, a subsequent question asked their relative position and field with respect to their organization, with the largest group of respondents (at 49%) identified as information security executives. The next largest group of respondents (at 22%) defined as information security managers or supervisors, and the third largest group (at 9%) were identified as IT executives. The remainder of respondents included General Corporate Executives (5%), IT Manager or Supervisor (5%), General Corporate Manager or

Supervisor (5%), Other Business Unit Manager or Supervisor (4%), and Other Business Unit Executive (1%).

4.1 Priority of Preferences for the DoL CIM Tiers

In examination of the data with regard to the first research question: *What are the priority of preferences for entry-level cybersecurity professionals for each of the Tiers of the DoL CIM?* Table 2 shows that in general, all seven competencies in the Personal Effectiveness Tier were highly ranked on their scale of 1=not important to 7= very important for entry-level security employees. At the top, indicative of the security field is Integrity – defined as *"Displaying strong moral principles and work ethic"* [7]. Tables 3-7 demonstrate the remaining priorities by tier.

Table 2
Prioritization of Tier 1: Personal Effectiveness Competencies

Personal Effectiveness Competencies*:	**Mean**	**S.D.**	**N**
Integrity	6.81	.496	199
Dependability & Reliability	6.56	.647	199
Interpersonal Skills	6.29	.986	199
Adaptability & Flexibility	6.27	.893	198
Initiative	6.20	.936	199
Lifelong Learning	6.17	1.034	199
Professionalism	6.00	1.032	200

Table 3
Prioritization of Tier 2: Academic Competencies

Academic Competencies*:	**Mean**	**S.D.**	**N**
Critical & Analytic Thinking	6.71	.592	195
Communications	6.54	.676	194
Fundamental IT	6.43	.812	195
Reading	6.37	.784	196
Writing	6.13	.905	196
Science	5.10	1.356	193
Mathematics	4.86	1.461	194

Table 4
Prioritization of Tier 3: Workplace Competencies

Workplace Competencies*:	**Mean**	**S.D.**	**N**
Problem Solving & Decision Making	6.34	.904	190
Teamwork	6.27	.926	192
Working with Tools & Technology	6.03	.997	192
Creative Thinking	5.95	.986	191
Planning & Organizing	5.78	1.086	192

Table 4
Prioritization of Tier 3: Workplace Competencies

Workplace Competencies*:	**Mean**	**S.D.**	**N**
Business Fundamentals	5.08	1.305	190

Table 5
Prioritization of Tier 4: Industry-Wide Technical Competencies

Industry-Wide Technical Competencies*:	**Mean**	**S.D.**	**N**
Cybersecurity Technology	6.13	1.046	189
Information Assurance	5.88	1.180	188
Incident Detection	5.87	1.206	190
Incident Response	5.84	1.280	189
Risk Management	5.74	1.369	190

Table 6
Prioritization of Tier 5: Industry Sector Functional Area Competencies

Industry Sector Functional Area Competencies:	**Mean**	**S.D.**	**N**
Protect & Defend	5.88	1.258	182
Analyze Information	5.77	1.380	183
Investigate Threats	5.60	1.417	181

Table 6
Prioritization of Tier 5: Industry Sector Functional Area Competencies

Industry Sector Functional Area Competencies:	Mean	S.D.	N
Operate & Maintain Security	5.59	1.220	184
Collect Information & Operate Cybersecurity Process	5.35	1.422	184
Securely Provision System	5.19	1.445	184
Oversee & Govern Cybersecurity Work	4.68	1.826	180

4.2 Priority by Industry

Next an examination of the second research question *Do these preferences vary by industry, and if so which ones?* was conducted. As none of the competency scores in any of the tiers were normally distributed for all levels of industry, as assessed by a Shapiro-Wilk's test ($p > .05$), in lieu of the standard ANOVA, a Kruskal-Wallis (KW) test was performed as a non-parametric equivalent, not dependent on a normal distribution. The results of the KW test found that in only three competencies were the perspectives of the various industry groups, statistically different, *Personal Effectiveness – Lifelong Learning; Workplace-Business Fundamentals* and *Industry-Wide Technical-Incident Detection*. However, with the low N in many of these response groups, and the fact that only 3 out of 32 competencies showed statistical differences between industry groups, it is assessed that in general there are no statistical differences in priorities of competencies between industry groups.

4.3 Priority by Organizational State

The third research question of interest examined was *"Do these preferences for entry-level cybersecurity professionals vary by organizational size?"* Just as was the case with industry groups, as none of the competency scores in any of the tiers were normally distributed for all levels of organizational size, as assessed by a Shapiro-Wilk's test ($p > .05$), in lieu of the standard ANOVA, a Kruskal-Wallis (KW) test was performed as a non-parametric equivalent, not dependent on a normal distribution. The results of the KW test found that in only two competencies did the perspectives of the various organizational sizes vary significantly at the $p < .05$ level. These two variables, Personal Effectiveness – Interpersonal skills and Personal Effectiveness – Dependability & Reliability. The results indicate that Personal Effectiveness – Interpersonal skills would be most important in Small organization, followed closely by Medium-sized organizations, which makes sense given the close interactions within organizations consisting of smaller numbers of employees. For Personal Effectiveness – Dependability and Reliability, Medium-sized organizations had the highest rating, followed closely by Extremely large and small-sized organizations. Based on these findings, the study would conclude that in general there is no support for the premise that the cybersecurity competencies differ by organizational size.

5 DISCUSSION, CONCLUSIONS AND NEXT STEPS

With the breadth and depth available in cybersecurity focused programs across the U.S., it is difficulty to specify a single "one-size fits all" approach to curriculum focus or depth. The competencies promoted by the DoL CIM model, based on the NIST NICE cybersecurity workforce framework can provide a common language for programs and students to evaluate their various options. Only by appreciating the variety of needs in industry, government and academia can information security education truly provide the breadth and depth of workforce-ready future employees needed to stem the future shortages so widely reported.

The findings of this study could serve as the starting point for academic institutions to specify and select concentrations for their desired security programs and coursework. Of the five tiers the DoL CIM model is organized into, Tiers 3 and 4 are the most promising in terms of competency priorities that could and should be reflected back into current and proposed programs of study in Cybersecurity. Tier 5 represents the overall NICE Framework specialty area the degree programs are typically focused on, and thus are less flexible. However, Tier 4 represents specializations or concentrations which could be added to degree programs, while Tier 3 represents key skills that could be added to any Cybersecurity, IS or IT course.

Additional research is needed to expand upon the Competencies and better understand the industry needs now and into the future.

REFERENCES

[1] (ISC)2, "(ISC)² Cybersecurity Workforce Shortage Continues to Grow Worldwide, to 1.8 Million in Five Years," Viewed 3/15/2018 from https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/02/13/Cybersecurity-Workforce-Shortage-Continues-to-Grow-Worldwide, 2017.

[2] Bureau of Labor Statistics, "Information Security Analysts," Viewed 3/10/2018 from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm, 2018.

[3] Bureau of Labor Statistics, "Computer and Information Systems Managers" Viewed 3/10/2018 from https://www.bls.gov/ooh/management/computer-and-information-systems-managers.htm, 2018.

[4] Pawlowski, S. and Jung, Y., "Social Representations of Cybersecurity by University Students and Implications for Instructional Design," Journal of Information Systems Education, 26(4): 281-294, 2015.

[5] Harris, M. and Patten, K., "Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum," Journal of Information Security Education, 26(3): 219-229, 2015.

[6] Newhouse, B., Keith S., Scribner, B. and Witte, G., "NICE Cyberscurity Workforce Framework (NCWF)," NIST Draft Special Publication 800-181. Viewed 5/15/2017 from http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf, 2016.

[7] Department of Labor, "Cybersecurity Industry Model" Viewed 7/26/2016 from (http://www.careeronestop.org/CompetencyModel/competency-models/cybersecurity.aspx), 2014.

[8] Kritzinger, E. & Smith, E., "Information security management: An information security retrieval and awareness model for industry," Computers & Security, 27(5-6): 224–231, 2008.

[9] Crossler, R.E., Johnston, A.C., Lowry, P. B., Hu, Q., Warkentin, M. & Baskerville, R., "Future directions for behavioral information security research," Computers & Security, 32: 90–101, 2013.

[10] Mullins, B.E., Lacey, T.H., Mills, R.F., Trechter, J.M. and Bass, S.D., "How the cyber defense exercise shaped an information-assurance curriculum", IEEE Security and Privacy, 5(5): 40-49, 2007.

[11] Malladi, S., El-Gayer, O. and Streff, K., "Experiences and lessons learned in the design and implementation of an information assurance curriculum," in Proceedings

of the 2007 IEEE Workshop on Information Assurance, United States Military Academy, West Point, 20-22 June, pages 22-29, 2007.

[12] Dark, M., Ekstrom, J. and Lunt, B., "Integrating Information Assurance and Security into IT Education: A Look at the Model Curriculum and Emerging Practice," Journal of Information Technology Education, 5(1): 389-403, 2006.

[13] Hentea, M., Dhillon, H.S. and Dhillon, M., "Towards changes in information security education," Journal of Information Technology Education, 5(1): 221-233, 2006.

[14] Katz, F., "The effect of a university information security survey on instruction methods in information security" in Proceedings of the 2nd Annual Conference on Information Security Curriculum Development. Kennesaw, Georgia: September 23–24, 2005, InfoSecCD '05. ACM, New York, NY, pages 43–48, 2005.

[15] Rezgui, Y. & Marks, A., "Information security awareness in higher education: An exploratory study," Computers & Security, 27(7-8): 241–253, 2008.

[16] Stewart, G. & Lacey, D., "Death by a thousand facts: Criticising the technocratic approach to information security awareness," Information Management & Computer Security, 20(1): 29–38, 2012.

[17] Ahmad, A. and Maynard, S., "Teaching information security management: reflections and experiences," Information Management & Computer Security, 22(5): 513 – 536, 2014.

[18] Vance, A., Siponen, M. and Pahnila, S., "Motivating IS security compliance: insights from habit and protection motivation theory," Information & Management, 1(2): 99-110, 2012.

[19] ABET, "Criteria for Accrediting Computing Programs: Effective for Reviews During the 2016-2017 Accreditation Cycle," Viewed 3/23/2018 from http://www.abet.org/wp-content/uploads/2015/10/C001-16-17-CAC-Criteria-10-20-15.pdf, 2016.

[20] Manson, D., Curl S. and Torner, J., "A Framework for Improving Information Assurance Education," Communications of the IIMA, 9(1): 79-90, 2009.

[21] Wilson, M. & Hash, J., "Building an information technology security awareness and training program," NIST Special Publication 800-50, Viewed 5/15/2017 from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf, 2003.

[22] Sauls, J. and Gudigantala, N., "Preparing Information Systems (IS) Graduates to Meet the Challenges of Global IT Security: Some Suggestions," Journal of Information Systems Education, 24(1): 71-73, 2013.

[23] Sharma, S.K. and Sefchek, J., "Teaching information systems security courses: a hands-on approach," Computers & Security, 26(4): 290-299, 2007.

[24] Bishop and Frinke, "Achieving learning objectives through E-voting case studies,", Security & Privacy, 5(1): 53-56, 2007.

[25] Ahmad, A., Ruighaver, A.B. and Teo, W.T., "An information-centric approach to data security in organizations," in Harris, R. (Ed), Proceedings of Tencon 2005: 2005 IEEE Region 10. 1-5, Swinburne University, Melbourne, 2005.

[26] Soomro, Z., Shah, M. and Ahmed, J., "Information security management needs more holistic approach", International Journal of Information Management: The Journal for Information Professionals, 36(2): 215-225, 2016.