Journal of the Midwest Association for Information Systems (JMWAIS)

Volume 2020
Issue 2 *Special Issue - Information Security, Privacy, and Ethics*

Article 5

2020

Alignment of Coursework with Knowledge Requirements: A Textbook Content Analysis

Mark Weiser
Oklahoma State University, weiser@okstate.edu

Andrew Bowman
andy.bowman@okstate.edu

Journal of the Midwest Association for Information Systems

Volume 2020 | Issue 2 Article 5

Date: 07-31-2020

Alignment of Coursework with Knowledge Requirements: A Textbook Content Analysis

Mark Weiser
Oklahoma State University, weiser@okstate.edu

Andy Bowman
Oklahoma State University, andy.bowman@okstate.edu

Abstract

Every information systems professional has a role to play in security. Analysts must consider security in their analyses and designs; programmers think through logic flaws that create vulnerabilities; and database managers need to provide appropriate access without exposing sensitive information to bad actors. Other disciplines also recognize the importance of employees having a respect for security and a broad understanding of concepts that enable it. Universities prepare students for careers across different domains; and the increasingly important formation of security knowledge falls to IS faculty. This study first examines relevant job postings to determine the knowledge, skills, and abilities most sought after by employers; then uses those results in a content analysis of current information security textbooks to indicate the degree to which employer-demanded concepts are covered in university-deployed teaching materials. The overall results of this study found that coverage of terms associated with security knowledge areas demanded by the marketplace is mixed among six leading textbooks, ranging from near complete coverage to just over half of the topics.

Keywords: *Content Analysis; Information Security Education; Textbook Analysis; Curriculum*

DOI: 10.17705/3jmwa.000061

1. Introduction

There is an extreme shortage of cybersecurity skills available in the U.S. workforce. In recent annual surveys by the Enterprise Strategy Group (ESG), in each of the last five years an increasing number of organizations reported "a problematic shortage of cybersecurity skills," with well over 50% in the most recent survey (Oltsik, 2019). U.S. News ranks Information Security Analysts 5th in all technology jobs, 19th in STEM, and 38th among the 100 best jobs in any field (U.S. News & World Report, 2020). Several job titles that rank even higher in surveys have information security knowledge as a basic requirement. CNNMoney/Payscale categorizes positions slightly differently but puts Information Assurance Analyst at number 5 among all job types (Braverman, 2017). Both rankings cite a median salary in excess of $98,000 with a bachelor's level education, compared to an overall IS salary average of $81,000 based on these same sources.

It's clear that demand for security knowledge far exceeds the number of appropriately-trained graduates with relevant four-year degrees. Many suggest that in order to bridge this gap, industry must turn to applicants with non-traditional backgrounds and even provide training to transition to this field (Zadelhoff, 2017). There is some question, however, if the general information security coursework provided by universities even covers the basic body of knowledge needed in entry-level positions.

It has become an expectation that IS programs incorporate security as a core component, as a separate course, or as modules embedded in multiple offerings across the curriculum. Other disciplines have recognized the importance of information security in their own career fields and have begun to offer required or optional coursework to build security awareness before entering the job market (Weiser & Conn, 2017). There is no agreement, however, about appropriate topics, depth, or scope for either the security practitioner or those for whom a broad understanding is sufficient. Because academia strives to place graduates in the most competitive positions, industry advisory boards comprised of prospective employers help educators shape topics. Recruiters, however, vary in opinion about the best direction in a constantly evolving field. Some employers turn to professional security certifications for affirmation that a job candidate has appropriate knowledge; but certifying bodies and training companies abound and do not agree on the set of desirable knowledge, skills, and abilities. The IS security field lacks a single unifying coordinating body upon which industry and academics can agree. Without accepted common topics and metrics like accountants have from the AICPA (AICPA, 2020), it is difficult to assess the degree to which information security curriculum offered in higher education, or tested by security certifications, actually matches the needs of the workforce.

This study analyzes relevant textbooks that provide a broad overview of information security; as indicated on the author's statements, publisher's marketing material, or the introduction to the book. These books are most often intended for second- or third-year bachelor's degree candidates who may then study information technology more broadly, or explore more depth in security during their upper-level courses. Although the same texts could be used for more advanced study, our scope is to explore the alignment of IT security knowledge for entry-level positions with the preparation that higher education provides.

Although a textbook certainly does not equate to the content of a course, it is a reasonable assumption that the book significantly influences the topics covered in the course. Content analysis of textbooks has been used for a variety of purposes across all fields of study. It can be used to gauge how long an emerging topic takes to appear in mainstream texts (Laksmana & Tietz, 2008); for comparative analyses of readability (Bargate, 2012); to indicate levels to which specific topics are covered; or even to identify different approaches to the same topics in different books (Foxman and Easterling, 1999; Fisher and Southey, 2005). Most commonly, however, textbook content analysis seeks to determine coverage of selected topics. Bracken and Urbancic (1999) analyzed ethics coverage in Accounting books, DeSensi & Jurs (2017) evaluated the presentation of psychological disorder stigma in Psychology texts, and Polikoff (2015) assessed the extent to which Mathematics textbooks meet common core standards.

To accommodate for the lack of an official knowledge list, this study systematically examines major job listing websites for terms most closely associated with information security knowledge. Because some positions referenced major professional certifications in lieu of, or in addition to, enumerating knowledge, skills, and abilities (KSAs) for candidates; content from those certifications was used to augment the list of KSAs. The superset of those words and phrases was then applied in an analysis of tables of contents from six major information security textbooks for inclusion of the concepts most sought by employers.

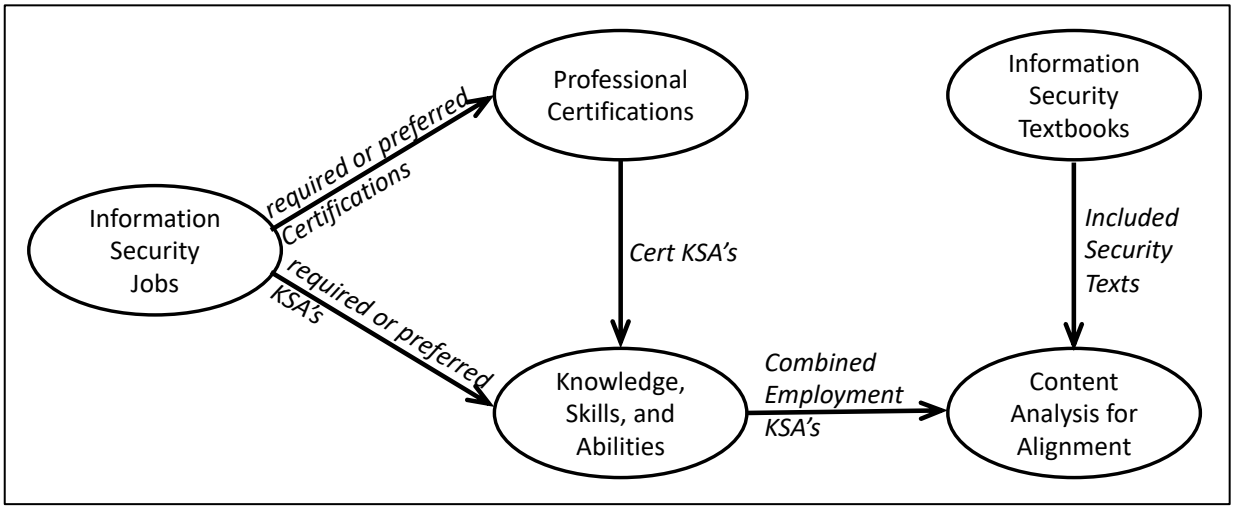
2. General Methodology

Content analysis is a systematic technique for representing longer passages of text into fewer content categories based on explicit coding rules (Berelson, 1952; Krippendorff, 1980). Holsti (1969) expands its application to include "any technique for making inferences by objectively and systematically identifying specified characteristics of messages." The most common application of content analysis is a word-frequency count, under the assumption "that the words that are mentioned most often are the words that reflect the greatest concern" (Stemler, 2000).

The lack of an accepted topic set for information systems security, as one may find for accounting or mathematics domains; however, means that we must first establish a set of knowledge objectives before gauging whether each is covered. A lack of common terminology and sub-topics further confounds this effort, so we employed the approach shown in Figure 1 to determine a non-redundant set of knowledge, skills, and abilities (KSAs) and then assess the presence of each in leading textbooks. We specifically:

1. searched relevant listings in multiple major job boards for KSAs and professional certifications that are required or preferred by prospective employers;
2. identified KSAs included in required or preferred professional certifications;
3. identified current textbooks with broad coverage in information security that could be taken by students without technical pre-requisites; and
4. analyzed textbook tables of contents to determine inclusions for job-driven KSAs.

Figure 1. Developing KSA's and Textbooks for Analysis



3. Task Methodology and Results

The scope of this study is to evaluate the alignment of security KSAs in entry-level positions with the content of textbooks used in IT security survey courses. To accomplish this, it was necessary to apply content analysis in three steps, each with a specific, objective and systematic approach. The first identified terms that represent knowledge skills and abilities required in relevant entry-level job postings. Because some postings referenced one or more security certifications rather than enumerating terms, we systematically determined representative KSA terms from those certifications. Finally, the most prevalent term from those two steps were used to objectively evaluate the content alignment in leading textbooks. Additional details of each process and the results follow.

3.1. Identification of KSA's and Certifications from Public Position Postings

Based on a Silk Road study involving the source of hired talent within corporations, ten top job search sites were identified (Research and Markets, 2016; Silk Road, 2016). Documentation of the query method employed by each site was reviewed and practical test queries were run to ensure that our systematic study process yielded objective and consistent results without redundancy that would skew results. Websites that require users to login were eliminated because the information gathered during the account creation process (skills, education, and location) was used to tailor results to the user. The biased results lead to a narrowed sampling of job listings that was not representative of entry-

level positions across the country. Other sites were excluded due to limiting the number of results per search, searches returning only local job listings, or use of semantic searches that lead to the number of results increasing for every additional word in the search, rather than refining the results. The table below details the reasons for excluding or including each site.

Table 1. Website Elimination Reasons

Website	Eliminated	Date Searched	Reason Eliminated
Glassdoor	Y	1/27/2020	Required login to search job listings
CareerBuilder	Y	1/27/2020	Limited search results to 5,000
Monster	Y	1/28/2020	More than three terms leads to increasingly large results
Simply Hired	Y	1/28/2020	More than two key terms leads to increasingly large results
Dice	Y	1/28/2020	Same jobs posted on other sites, introducing redundancy in data
Snagajob	Y	1/29/2020	Location based searches required
Indeed	N	1/27/2020	
Monster	N	1/29/2020	
Zip Recruiter	N	1/30/2020	
Google for Jobs	Y	1/27/2020	Focus on job postings

The first search used the term "Information Security," without any location preference. From among many relevant security-related searches, this term was selected because it returned the highest number of results of which at least 70% were identifiable as jobs within the domain of interest. A Boolean "AND" was used between terms on sites where necessary to return positions that included all terms in any section of the position description.

Each listing was reviewed in the order returned from the search and was first assessed for relevance to the domain and applicability for the purpose of this study. A position announcement was excluded from further review if:

- The job was not primarily in information security: eliminated secretarial jobs which required maintaining "privacy" of records, janitorial positions that listed a need "securing the site," and other references that fell outside of the scope of this study.
- More than two years of work experience was required: the scope of this study includes positions for which undergraduate study was the main preparation.
- A top-secret or higher clearance was required: the majority of these positions required specific experience such as prior military or government service which put it outside of the scope of this work.
- It was a temporary position, such as an internship or contract-based work: many of these occur before undergraduate study is complete.

If not eliminated, the position listing was reviewed in detail and KSAs and/or professional certifications that were required or preferred were recorded. Every job listing that fit the criteria was checked against all previously recorded job listings to ensure that no redundant postings were included. This process was repeated until KSAs and certificates from five non-eliminated position listings were recorded. Similar or highly related terms were consolidated, for instance "cloud", "cloud security", and "cloud architecture" were grouped into "cloud" and all subsequent cloud references were considered equivalent.

Because the different search engines vary significantly in size, we normalized the data by dividing the number of positions returned from each search by the number of positions returned by the search for only "information security" alone. This ratio for each KSA is recorded in Table 2 and ordered from highest to lowest by the sum of the ratios from all three included job search sites. The top twenty terms that were not direct references to names of professional certifications were retained to be used in further analysis as representative of knowledge areas that are most important in the field of information security.

Table 2. Top KSA terms from relevant position listings

Information Security…	Indeed	LinkedIn	Zip	Score
Risk	.1926	.0927	.1505	**.436**
Cloud	.0966	.1391	.1593	**.395**
Windows	.1036	.1060	.0822	**.292**
Networking	.0654	.0861	.0836	**.235**
Database	.0686	.0199	.1267	**.215**
Linux	.0621	.0795	.0639	**.205**
Mobile	.0574	.0596	.0632	**.180**
Vulnerability	.0441	.0728	.0329	**.150**
Web Application	.0673	.0331	.0405	**.141**
Active Directory	.0238	.0331	.0443	**.101**
Firewall	.0339	.0265	.0400	**.100**
Scripting	.0388	.0066	.0488	**.094**
Unix	.0248	.0397	.0294	**.094**
Security Standards	.0175	.0265	.0313	**.075**
Coding	.0297	.0063	.0315	**.068**
Patch	.0185	.0132	.0305	**.062**
Encryption	.0132	.0265	.0167	**.056**
Intrusion Detection/Prevention	.0120	.0265	.0165	**.055**
API	.0134	.0132	.0234	**.050**
SIEM	.0103	.0265	.0124	**.049**

Each job posting had a unique structure and employed varying terminology, so subjectivity in the analysis was necessary to convey results with practical importance that still retain objective comparable numeric measures. In some cases, terms were combined during the process. For instance, "encryption" and "decryption" either appeared together in most of the reviewed position descriptions or knowledge of both areas was implied. Based on the reviewed sets, the number of unique positions that included either or both terms were extrapolated to form the total for that combined topic. Similarly, "intrusion detection" and "intrusion prevention" were combined. "Scripting" and "coding;" however, were left as separate terms because the context of many reviewed positions appeared to use "coding" for more complex programming of full applications, whereas "scripting" in the security domain often referenced shorter segments to tie together processes and automate tasks. The use was inconsistent and each was sufficiently prevalent that, whether the terms were treated separately or collectively, both would be represented in our final results.

Many position descriptions included a preference that candidates had one of several professional certifications, with fewer having them as a requirement. Within the 50 most frequent terms during the job posting search, 13 were references to certifications in the IS security industry, including the five top certifications according to the ISSA (Oltsik, 2019). These certifications are awarded by professional organizations for individuals who can take a test proving knowledge and/or competence in information security areas. A review of the official website for each certification allowed us to delve deeper into the topics covered.

Appending the certification name to the term "information security" in the same way as was done previously, we recorded the number of positions returned by the job search sites and scored them in the same way described in our KSA discovery process. The results are in Table 3 and are ordered with the certification that is most referenced by position listings (CISSP) to the least (GCED). It should be noted that Security+ appeared in many position descriptions; however, it was not included in the table because the highly varied ways that the search engines processed a "+" prevented a comparable metric to be computed for that certification. There were also references to categories of certifications, such as "GIAC" which indicates the group of all SANS certifications, so the collective term GIAC was omitted in favor of individual certification names.

Table 3. Top certifications from relevant position listings

Information Security…	Cert Org	Indeed	LinkedIn	Zip	Score
CISSP	$(ISC)^2$	.0349	.0530	.0345	**.122**
CISA	ISACA	.0154	.0331	.0176	**.066**
CISM	ISACA	.0121	.0331	.0009	**.046**
CEH	EC-Council	.0074	.0132	.0005	**.021**
GSEC	$(ISC)^2$	.0060	.0132	.0004	**.020**
SSCP	$(ISC)^2$	.0063	.0066	.0003	**.013**
GCIH	GIAC	.0047	.0066	.0003	**.012**
CASP	CompTIA	.0047	.0066	.0003	**.012**
OSCP	Offensive-Sec	.0027	.0066	.0002	**.010**
GCIA	GIAC	.0020	.0057	.0002	**.008**
GPEN	GIAC	.0016	.0051	.0002	**.007**
GCED	GIAC	.0021	.0046	.0001	**.007**

3.2. Identification of Additional KSA's From Certifications found in Public Position Postings

Some employers listed required or preferred professional certifications in lieu of enumerating KSAs expected of a successful candidate, others stated desirable knowledge areas, and some included both. The implication is that a company listing professional certifications is seeking the knowledge demonstrated by a candidate to obtain that certification. In order to capture additional KSAs which were not revealed by the term search in Table 2, we reviewed the publicly available topic list for each certificate in Table 3, in addition to Security+, which was omitted from the table because of search anomalies described previously. The topic list for each certification, as presented on the official website for each ((ISC)2, 2020; CompTIA, 2020, EC-Council, 2020; ISACA, 2020; GCIA, 2020; Offensive Security, 2020) was reviewed for the presence of each of the terms that were drawn from our job search analysis.

Table 4 shows which topics appear in the knowledge list for each certification. Certifications are listed across the top are in order of their prevalence in position listings, as determined above. The "Job Appearance Score" shown for each is the taken from Table 3. Terms are sorted by the number of certifications in which each appears, as recorded in the right-hand column. Only terms that appeared in five or more certifications are shown. Six KSA terms that were not captured in our earlier job postings process appeared in at least five of the listed professional certifications, and those appear at the bottom of the table under the double line. "Penetration," for example, did not receive a sufficiently high score to appear in the results of our earlier process, but was identified by ten of the 13 professional certifications to which employers referred when searching for candidates. It is therefore assumed to be an important term that represents a KSA sought in future employees and is incorporated in our textbook content analysis. Similarly, "forensic tools", "control", "log", "auditing", and "client side / server side" (collectively) were included as relevant important terms in security education.

Table 4: KSA coverage indicated by certification topic list

Certification	CISSP	CISA	CISM	CEH	GSEC	SSCP	GCIH	CASP	OSCP	GCIA	GPEN	GCED	Sec+	count
Job Appearance Score	.122	.066	.046	.021	.020	.013	.012	.012	.010	.008	.007	.007		
Intrusion Det/Prev	X	X	X	X	X	X	X	X	X	X	X	X	X	13
Vulnerability	X		X	X	X	X	X	X	X	X	X	X	X	12
Networking	X			X	X		X	X	X	X	X	X	X	10
Malware	X				X	X	X	X	X	X	X	X	X	10
Firewall	X				X	X	X	X	X	X		X		8
Packet				X		X	X	X	X	X	X	X		8
Risk	X	X	X		X	X	X	X			X		X	9
Cryptography/Encrypt	X	X		X	X	X		X	X			X	X	9
Coding	X				X	X		X	X		X	X	X	8
SIEM	X	X	X		X	X	X					X	X	8
Web Application	X	X			X	X	X	X	X		X			8
Identity Management	X	X			X	X		X	X		X			7
Security Standards	X	X	X		X			X				X		6
Endpoint	X	X			X	X		X	X					6
Cloud	X				X	X		X				X		5
Database	X	X				X		X			X			5
Linux					X	X	X	X	X					5
Mobile	X	X			X			X	X					5
Penetration	X	X		X	X	X	X		X		X	X	X	10
Forensic Tools	X	X		X			X	X	X	X				7
Control	X	X		X	X		X	X	X					7
Log	X			X	X		X	X		X				6
Auditing	X	X		X	X	X		X						6
Client side / Server Side					X	X	X	X	X					5

3.3. Identification of Leading Relevant Textbooks

This analysis focuses on textbooks that are actively being used in overview courses in Information Security and are neither highly technical nor have significant pre-requisites. The authors first reviewed leading academic publishers' catalogs for textbooks in this domain which are currently being marketed in higher education settings. 15 titles were identified. For each book, the publisher's marketing material and authors' notes were reviewed to glean the type of class and student for which it was intended. Textbooks that were for advanced students, focused on a specific sub-domain of security or technology, or were published before 2016 were eliminated from further analysis. As a confirmation of the final selected set, we located 20 syllabi from general information security courses taught in the most recent academic year; each at a comprehensive 4-year university. None of the courses employed a textbook that was not on our original list, although two used texts that we had eliminated; one because it was an older edition, and the other because it focused on a more specific sub-domain of the field, putting it outside of this study's scope.

The remaining six textbooks had copyright dates of 2016 or newer and spanned four publishers and five authors. (Ciampa, 2016; Easttom, 2019; Smith 2019; Vacca, 2017; Whitman and Mattord, 2017; Whitman and Mattord, 2018). These six books are the subject of a content analysis for alignment to KSAs identified in position announcements.

3.4. Content Analysis of Textbooks for Alignment to KSA's from Current Position Postings

A detailed table of contents (TOC) was obtained for each of the six textbooks to be studied. For some publishers, the full text of the most current edition was available and the combined detailed outlines of each chapter was used. For others, a detailed TOC that spanned the entire textbook was accessible. In each case, the reviewed material included the highest-level subject and at least two levels of sub-topics below. This level of detail gave the authors of this study sufficient granularity to determine subject areas that were important enough or covered in adequate detail, without using the index which would have references to terms that may have simply been used or defined in the text.

Table 5. KSA Presence in TOC of Textbooks

KSA Term	T1	T2	T3	T4	T5	T6	#
Active Directory	x	x	x	x	x	x	6
Auditing	x	x	x	x	x	x	6
Cryptography/Encryption	x	x	x	x	x	x	6
Firewall	x	x	x	x	x	x	6
Intrusion Det/Prev	x	x	x	x	x	x	6
Log	x	x	x	x	x	x	6
Networking	x	x	x	x	x	x	6
Risk	x	x	x	x	x	x	6
Security Standards	x	x	x	x	x	x	6
Vulnerability	x	x	x	x	x	x	6
Patch	x	x	x	x	x	x	6
Client side / Server Side	x	x	x	x	x		5
Control	x	x	x	x	x		5
Endpoint	x	x	x	x		x	5
Forensic Tools	x	x	x	x	x		5
Identity Management	x	x	x	x	x		5
Mobile	x	x	x	x		x	5
Packet	x	x	x	x	x		5
Web Application	x	x	x	x		x	5
Malware	x		x	x		x	4
Penetration	x		x	x			3
Scripting	x		x			x	3
Windows	x	x	x				3
Database	x	x					2
Linux	x	x					2
SIEM	x	x					2
Unix	x	x					2
Cloud		x					1
Coding	x						1
API							0
	28	25	23	21	16	16	

For each KSA term in the superset from Table 2 and Table 4, a search on the detailed TOC was performed. The presence or absence of each term, or a close derivation of it, was then recorded. The results of this analysis are presented in Table 5. The first column shows the KSA term as discovered either in position descriptions on major job search sites, or in detailed content descriptions of certifications that appeared in job descriptions. The "T" columns indicate the presence of a term in one of the six textbooks. Textbook 1 (T1) the Smith (2019) textbook, T2 stands for the Vacca (2017) textbook, T3 indicates the Easttom (2019), T4 represents the Whitman and Mattord (2017) Principles book, T5 is the Whitman and Mattord (2018) Management book, and T6 is the Ciampa (2016) book. The last column shows the number of textbooks in which each term was located and the last row indicates the number of these terms that appears in that book. KSA terms are ordered from top to bottom beginning with the terms that appear in all textbooks. Texts are ordered from left to right beginning with the one which includes the most KSA areas.

Coverage of the areas is inconsistent across the textbooks, as indicated by the tables of contents. The first 10 KSA terms (33%) appeared in all six of the textbooks and 19 of them (63%) were addressed in at least four of the six texts. The remaining 10 KSA terms (33%) appeared in half or fewer of the reviewed textbooks, including "API" which was not explicitly mentioned in any table of contents from the textbooks.

4. Discussion, Limitations, and Conclusions

Although academia strives to educate students with knowledge, skills, and abilities that are demanded by employers; faculty perceptions of relevant topics may not align with industry requirements. In rapidly evolving fields like information security this problem can be particularly acute; with new topics constantly emerging, others becoming less important; and some transforming to the extent that they require entirely different approaches to understand. Because of this reality, instructors rely on textbooks authors to heavily influence the propriety of topics covered. Textbook authors, however, also face the same impediments in this dynamic field and are constrained by lengthy revision cycles of traditional publishers.

Because of the rapidly changing nature of information security, it might be expected that inclusion of knowledge topics currently demanded by the job market is strongly related to the publication date of the textbook. Indeed, the book with the most recent publication date (Smith, 2019) did include the most terms, however, it lacked "cloud" within the table of contents. This area has received growing attention in the IS community, particularly with respect to security, yet the only textbook that treated it with sufficient weight to appear in the table of contents was the second oldest of the textbooks (Vacca, 2017). In fact, a full-text search of two of the textbooks and their indices did confirm a lack of coverage in those books. It is important to recognize possible omissions such as these to ensure graduates who have taken even an overview course in information security understand the high-level issues.

An important contribution of this study is to draw attention to potential misalignment between areas of knowledge that are important in the information security industry, but that may not appear in popular textbooks intended to broadly cover the field. Instructors may use supplemental materials to cover any omissions; determine that the general security knowledge is sufficiently applicable to a specific omitted term; relegate coverage to a future course; or simply favor other topics. With limited resources, trade-offs may be necessary and this study assists in identifying potential problematic areas.

The authors performed a content analysis on textbooks as a surrogate for class content, because textbooks are more readily available than detailed syllabi or course outlines. The implicit assumption is that the content of a textbook has a significant influence over any course in which it is used. In many cases this is true; however, the authors recognize and accept that there are differences between formal materials and knowledge acquired within any course. Even if a topic has been identified by this study, some areas could be minimized or omitted in an introductory textbook with the expectations that later courses will cover them in more depth. It is also likely that there are so many potential subject areas in this field, that authors intentionally focus on a subset of areas to build a general awareness and competence.

It is also an unfortunate reality that in excess of 60% of university students do not purchase at least one of their required textbooks in a given term (Hilton, 2016; Martin et al., 2017). Students cite high cost and lack of alignment with exams and job aspirations. It can certainly be argued that students do not have a firm basis to know requirements for future jobs, so the burden falls to instructors to assure that selected textbooks and other content aligns well with actual job requirements to better justify the benefit that investment in a textbook has to students' career potential.

The process this study employed to determine the most important current and relevant knowledge, skills, and abilities is itself a contribution. Any highly dynamic academic discipline that lacks an official governing body to specify and revise expected knowledge requirements could benefit from this approach. In fact, the authors of this study recognize that it is highly likely that the specific terms identified may not appear if the study were replicated in the future. That does not diminish the value of the outcomes but highlights the need for a rigorous approach to assist in topical alignment between industry demands and academic offerings. A benefit of this simple cyclical method is that there appears to be a high level of convergence in terms within as few as 30 position announcements from two non-overlapping job search engines, making it very practical to replicate or apply elsewhere.

While professional certification review was an intermediate step in this study, we included the full results table because it contributes value in its own right. Out of the certifications explored, two of the top three certifications, CISA and CISM focus on management aspects of information security but lack direct mentions to many of the listed KSAs both are considered among the most important certifications to achieve for an information security job (Oltsik, 2019). This highlights the importance of both the technical and managerial aspects of security, as well as potential career paths for those able to manage projects and organizations, but who may not have the depth and breadth of technical detail.

It may also appear that using jobs specifically in the information security field to derive a set of KSAs for a general survey course is inappropriate. The study of job postings, however, was done to extract a set of the most critical issues facing companies today. The analysis of the textbooks, however, only revealed the presence of topical coverage, rather

than a measurement of depth. It is reasonable that an awareness-level coverage of the most pressing topics in a field be included, or that the instructor makes an informed decision to omit one or more areas.

Summing weighted results from multiple job sites could be considered overly simplistic. There is not an accepted method to determine unspecified inclusion terms for a textbook content analysis and other approaches were considered for this study. For instance, terms extracted from certification details could then have been multiplied by the Job Appearance Score, incorporating how often a certificate is referenced in a job announcement. The approach we used was more inclusive, significantly easier to understand, and met the guidelines for content analysis.

There are a few limitations in the content analysis itself that should be noted. First, this analysis only reviews six popular information security books. Although each is used by multiple universities for general coverage of information security, they do not represent the entire set of such textbooks. The study authors did, in fact, identify some university offerings that used other books. Second, a comprehensive search of the full text was not performed. The content analysis was done on a detailed table of contents for each book and the level of detail varied between authors and publishers. It is very likely that some of these terms appear within the full text, but the concept was not prevalent enough to appear in the table of contents. Third, although the study authors were diligent in the reviews and have sufficient experience in the domain to identify similar terminology to not unnecessarily exclude a text from the table, it is possible that some instances of KSA terms went undetected, or terminology was not similar enough to be recognized.

Finally, there is a need for a study more closely relating actual course content to information security positions. This study used textbook content as a surrogate for course coverage. A more direct review of detailed syllabi and course outlines would better reveal the degree to which higher education is addressing the needs of industry, creating the impetus for change and continuous improvement across the discipline.

4. References

(ISC)2. (2020) (ISC)2 Information Security Certifications. Retrieved from https://www.isc2.org/Certifications

AICPA. (2020). Association of International Certified Professional Accountants. Retrieved from https://aicpa.org

Bargate, K. (2012). The readability of managerial accounting and financial management textbooks. Meditari Accountancy Research, 20(1), 4-20.

Berelson, B. (1952). Content Analysis in Communication Research. Glencoe, Ill: Free Press.

Bracken, R. M., & Urbancic, F. R. (1999). Ethics content in introductory accounting textbooks: An analysis and review. Journal of Education for Business, 74(5), 279-284.

Braverman, B. (2017, May 9). Best Jobs in America. Retrieved from https://money.cnn.com/gallery/pf/2017/01/05/best-jobs-2017/5.html

Ciampa, M. (2016). Security Awareness: Applying Practical Security in Your World (5th ed.). Boston, MA: Cengage Learning.

CompTIA. (2020). CompTIA Security+. Retrieved from https://comptia.org/certifications/security

DeSensi, V. L., & Jurs, B. S. (2017). Coverage of Psychological Disorder Stigma in Introductory Psychology. North American Journal of Psychology, 19(3).

Easttom, C. (2019). Computer Security Fundamentals (4th ed.). London, UK: Pearson.

EC-Council. (2020). Certified Ethical Hacker. Retrieved from https://cert.eccouncil.org/certified-ethical-hacker.html

Fisher, C. D., & Southey, G. (2005). International human resource management in the introductory HRM course. The International Journal of Human Resource Management, 16(4), 599-614.

Foxman, E., & Easterling, D. (1999). The representation of diversity in marketing principles texts: An exploratory analysis. Journal of Education for Business, 74(5), 285-288.

GIAC. (2020). Cybersecurity Certifications. Retrieved from https://giac.org/certifications

Hilton, J. (2016). Open educational resources and college textbook choices: a review of research on efficacy and perceptions. Educational Technology Research and Development, 64(4), 573-590.

Holsti, O. (1969). Content Analysis for the Social Sciences and Humanities. Reading, MA: Addison-Wesley.

ISACA. (2020) ISACA CREDENTIALS. Retrieved from https://www.isaca.org/credentialing

Krippendorff, K. (1980). Content Analysis: An Introduction to Its Methodology. Newbury Park, CA: Sage.

Laksmana, I., & Tietz, W. (2008). Temporal, cross-sectional, and time-lag analyses of managerial and cost accounting textbooks. Accounting Education: an international journal, 17(3), 291-312.

Martin, M., Belikov, O., Hilton, J., Wiley, D., & Fischer, L. (2017). Analysis of student and faculty perceptions of textbook costs in higher education. Open Praxis, 9(1), 79-91.

Polikoff, M. S. (2015). How well aligned are textbooks to the common core standards in mathematics?. American Educational Research Journal, 52(6), 1185-1211.

Offensive Security. (2020). Course Overview. Retrieved from https://www.offensive-security.com/pwk-oscp/

Oltsik, J. (2019). The life and times of cybersecurity professionals. ESG and ISSA: Research Report. Retrieved from https://www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf

Research and Markets (2016). United States Online Recruitment Market 2016 – 2020 with LinkedIn, CareerBuilder, Monster & Indeed Dominating. PR Newswire.

Silk Road. (2016). Top Sources of Hire 2016. Retrieved from http://hr1.silkroad.com/source-of-hire-report-download

Smith, R. E. (2019). Elementary Information Security (3rd ed.). Burlington, MA: Jones and Bartlett Learning.

Stemler, Steve (2000) "An overview of content analysis," Practical Assessment, Research, and Evaluation, 7(17).

US News & World Report. (2020). Information Security Analyst Overview. Retrieved from https://money.usnews.com/careers/best-jobs/information-security-analyst

Vacca, J. R. (2017). Computer and Information Security Handbook (3rd ed.). Burlington, MA: Morgan Kaufmann Publishers.

Whitman, M. E., Mattord, H. J. (2018). Management of Information Security (6th ed.). Boston, MA: Cengage Learning.

Whitman, M. E., Mattord, H. J. (2017). Principles of Information Security (6th ed.). Boston, MA: Cengage Learning.

Weiser, M., & Conn, C. (2017). Into the breach: Integrating cybersecurity into the business curriculum. BizEd, 16(1), 36-41.

Zadelhoff, M. V. (2017). Cybersecurity has a serious talent shortage. Here's how to fix it. Harvard Business Review. Retrieved from https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it

Author Biographies

Mark Weiser is a Professor of Management Science and Information Systems at Oklahoma State University. He has published in leading journals and proceedings, focusing on the areas of upper-layer network protocols, security, forensics, and technology-supported teaching. Dr. Weiser was founding director of the Center for Telecommunications and Network Security and principle investigator for funded projects from DoD, NSA, AFOSR, NSF, and multiple private agencies.

Andrew Bowman is a PhD Student studying Management Science and Information Systems at Oklahoma State University. His research interests include Digital Piracy, Digital Activism, and Consequences of Blockchain Technology and other Decentralized Applications.