Communications of the Association for Information Systems

Volume 39 Article 3

7-2016

Teaching Information Security in Business Schools: Current Practices and a Proposed Direction for the Future

W. Alec Cram
Bentley University, wcram@bentley.edu

John D'Arcy
University of Delaware

Recommended Citation
Cram, W. Alec and D'Arcy, John (2016) "Teaching Information Security in Business Schools: Current Practices and a Proposed Direction for the Future," *Communications of the Association for Information Systems*: Vol. 39 , Article 3.
DOI: 10.17705/1CAIS.03903
Available at: http://aisel.aisnet.org/cais/vol39/iss1/3

Communications of the Association for Information Systems

IS Education Paper ISSN: 1529-3181

Teaching Information Security in Business Schools: Current Practices and a Proposed Direction for the Future

W. Alec Cram
Department of Information and Process Management
Bentley University
wcram@bentley.edu

John D'Arcy
Department of Accounting & MIS
University of Delaware

Abstract:

The growing importance of information security as a business issue has encouraged instructors to extend their courses beyond a hands-on, technical model to one that considers managerial and risk-based issues. In business schools, this shift has presented the pedagogical challenge of balancing the technical content fundamental to information security with the managerial content that the profession increasingly values. To draw on the best practices currently being undertaken in the classroom, we examine 44 information security course syllabi from business and other schools (i.e., computer science, engineering, information science, law, and mathematics). Using a qualitative approach, we identify the definitive technical and managerial-focused aspects of information security courses. Based on the results, we propose an introductory information security course that balances technical and non-technical content for business school students and that integrates the most innovative techniques used by today's information security instructors.

Keywords: Information Security, Pedagogy, Curriculum, Course Development.

This manuscript underwent editorial review. It was received 09/24/2014 and was with the authors for 5 months for 2 revisions. Raj Sharman served as Associate Editor.

1 Introduction

Educators have traditionally viewed information security courses as highly technical and targeted towards students with an interest in designing, configuring, and operating security tools. From cryptography to malware and access control to steganography, non-business disciplines such as computer science and engineering have often taught such courses. However, these technically oriented security courses have expanded in recent years to consider the broader issues of the people, processes, and technology involved with information security (Hutchinson & Warren, 2002; Long & White, 2010; Whitman & Mattord, 2004). This transition reflects the increasing business focus of security education; indeed, a growing number of organizations now demand that employees understand security fundamentals related to business processes, regulatory compliance, and customer data (White, Hewitt, & Kruck, 2013). To address this demand, undergraduate and graduate programs in business schools are increasingly offering information security courses for students who specialize in non-technical disciplines such as accounting, finance, and marketing (Walters, 2007). Information security's shift from a primarily hands-on, technical course to an increasingly management-focused, risk-based course has resulted in a variety of pedagogical challenges, some of which we explore in this research.

In contrast to information security courses taught in computer science or engineering departments, instructors in business schools must face how technical the course should be. Recent job market analysis highlights the importance of not only technical knowledge but also managerial skills (ISC^2, 2013; Hulme, 2012; SANS Institute, 2014). Based on our experience in the classroom[1], we note that some business students have familiarity with programming, network design, and operating systems and would benefit from (and desire) an information security course that examines deep technical content; on the other hand, some students have little technical background and would prefer a course that instead focuses on the managerial aspects of information security. With a primarily technical course, our experience suggests that many non-technical business students feel threatened by such content and avoid enrolling in the class and, thereby, miss an opportunity to build the holistic body of security knowledge that employers demand; with a non-technical course, many students with a technical background feel that the course will not meet their expectations (i.e., "it's too soft"), enroll in other courses, and, thus, miss an opportunity to develop managerial-oriented knowledge related to security. Depending on the path taken (i.e., deciding how much to focus on the technical versus the managerial), instructors will need to select different course materials, design different assignments, and provide different class formats (e.g., case studies, tool demos, etc.).

Against this backdrop, we pose the following question:

> **RQ:** What current pedagogical practices can information security instructors in business schools employ to more effectively balance technical and managerial content in an introductory course?

We examine 44 information security course syllabi from classes that business and other schools (i.e., computer science, engineering, information science, law, and mathematics) offer. Using a qualitative, content-analysis approach, we identify the definitive aspects of these courses, including trends related to course materials, assignment design, and class format. Based on our results, we outline an introductory information security course that balances technical and non-technical content for business school students and that integrates the most innovative techniques that today's information security instructors use. Instructors representing both business and non-business schools could potentially co-teach this course; alternatively, a single instructor familiar with both disciplines could teach it

This paper proceeds as follows. In Section 2, we overview the information security discipline, including past research on pedagogical perspectives. In Section 3, we discuss our methodology and the approach we used to evaluate the collected syllabi. In Section 4, we present the results and outline our proposed course. In Section 5, we discuss the future of information security education in business schools. Finally, in Section 6, we conclude the paper.

[1] The first author has taught courses on information security and computer forensics (5 undergraduate sections), IT audit (8 graduate sections), and information security, controls, and ethics (2 graduate sections), whereas the second author has taught information security-related courses (network security, information assurance, IT risk management) for ten years (16 undergraduate sections; 10 graduate sections).

2 Teaching Security: The Fundamentals

Researchers have provided a variety of definitions and meanings for computer and information security. Denning, Parker, Nycum, and Ware (1984) broadly define computer security as "that body of technology, techniques, procedures, and practices, that provides the protective mechanisms to assure the safety of both the systems themselves and the information within them, and limits access to such information solely to authorized users" (p. 315). Landwehr (2001) suggests that computer security is more narrowly focused than information security. From this perspective, computer security has three main foci: 1) securing the data that one receives, stores, and retransmits; 2) securing the processes that one performs on these data; and 3) securing the physical system properties such as backup tapes, hard-copy output, and laptops (Landwehr, 2001).

Information security courses taught in computer science and engineering have traditionally focused on the first and third of these components (i.e., the formal, automated part of an information system). As such, these courses view information security as a technical issue that one can effectively manage by selecting appropriate hardware and software components and designing an architecture to protect the organization's information assets. However, as we note in Section 1, there has been a shift toward business-oriented information security courses. This shift reflects the growing recognition that information security is just as much a business issue as it is a technical one. Various industry surveys and reports (e.g., Ponemon Institute, 2013) document the substantial financial and reputational costs that organizations bear as a result of breaches to their information systems. Consequently, ensuring information security has become a top management priority in many organizations and in sectors of the U.S. Government. Further, many organizations now seek security professionals armed with latest knowledge and skills involving both the technical and managerial aspects of the domain (ISC[2], 2013).

Researchers have extensively documented the shortage of information security professionals (Bishop, 2006; Cisco, 2014; Morgan, 2015). Organizations have attempted to fill this void by recruiting employees from law enforcement and military and by developing employees' security skills in-house (Whitman & Mattord, 2004). However, most security advocates agree that the next generation of security professionals must come from programs of higher education (Andress, 2014a). As a result, formal information security curriculums are now a growing trend in many universities worldwide (Bradshaw, 2015). However, two issues prevent providing these courses to students: 1) the lack of consensus on the topical content of information security programs, and, 2) as the duplication of topics that we found in reviewing the business and non-business syllabi for this paper evidences, the question of which discipline can best cover the required technical and non-technical content. Echoing Foltz and Renwick's (2011, p. 124) views, we may now need to consider new approaches for teaching information security to increase both the breadth and depth of our students' educational experience.

The growing importance of information security in business has altered the highly technical focus of courses that computer science and engineering schools traditionally offered. Past pedagogical research has considered the approaches to design and deliver a broad security curriculum (Whitman & Mattord, 2004; Woodward, Imboden, & Martin, 2013), examined information security coverage in current courses (Foltz & Renwick 2011), and explored the techniques used to deliver technically oriented security education (Yurcik & Doss, 2001). Although security's managerial elements are fundamental in business school courses, they must introduce at least some introductory technical foundation. Finding a balance has resulted in challenges to administrators, course designers, and instructors. Though no one solution can determine the right technical-managerial balance for every school, we outline a business school-based information security course that finds a middle ground in a single, hybrid class. Because many schools offer a technical-based information security class already[2], the proposed course should avoid duplicating efforts and provide a distinct value for business students. Based on our combined experience teaching information security in business schools, we approach this research as an opportunity to contribute to ongoing improvements to courses in our discipline. In Section 3, we detail the methodological approach that we employed for this project.

[2] Readers can find an example syllabus from such a course at https://www.andrew.cmu.edu/course/14-761/S15%20AIA%20Syllabus.pdf

3 Methodology

We adopt an archival approach in reviewing course syllabi related to information security classes. To limit the source data to a manageable quantity, we focused our search to U.S.-based schools and to those syllabi that we could access online. We used search engine terms such as "information security syllabus" and "information assurance syllabus" to locate the documents. We collected a total of 44 information security syllabi: 20 from business school-based courses and 24 from non-business courses (including computer science, engineering, information science, law, and math)[3]. We included both undergraduate and graduate courses and a mix of traditional and online courses. The collected data comprised 265 total pages (i.e., an average of 6 pages per syllabus). Refer to Appendix A for a detailed listing of the source documents, including schools and course names. We provide additional descriptive details in Section 4. After collecting the available syllabi, we descriptively coded the documents, which refers to classifying segments of text as a particular phenomenon (Miles & Huberman, 1994). We coded the papers into both higher-level categories and a series of underlying subcategories (see Table 1). We established a preliminary set of categories at the beginning of the coding process based on the domains existing in two popular security certifications: the Certified Information Systems Security Practitioner (CISSP) and Certified Information Security Manager (CISM) (Hernandez, 2012; ISACA, 2014). The first author coded a preliminary sample of syllabi, which the second author reviewed. We discussed the initial approach and results and refined the categories. We then coded the remainder of the syllabi and, as we identified new characteristics in the data, iteratively defined the categories. By the end of the coding, we did not encounter any new coding categories, which suggests that we reached a saturation point in the taxonomy. We coded a total of 542 passages into four main categories and thirty subcategories (i.e., an average of 12 passages per syllabus). Appendix B provides representative examples of data coded to each category. We avoided going into a more granular layer in the subcategories to allow individual instructors a greater degree of flexibility in adapting our results. To further establish the artifact's validity, we provided a summary of our coding results to eight individuals with expertise in either information security practice or information security pedagogy. We asked them for feedback on the artifact in terms of our coding categories and subcategories. The participants provided a series of helpful suggestions, but they identified no substantive gaps. The results from this analysis allowed us to identify the key technical and managerial-oriented elements of information security courses and trends in class objectives, course materials, and student-evaluation techniques. During the coding, we also identified topics or pedagogical techniques that we viewed as distinctive and valuable. We discuss these topics and techniques in detail in Section 4.

In analyzing the data, we focused on identifying trends that could contribute toward developing an introductory information security course for business students that would effectively balance both technical and managerial content and also draw on the best practices and novel techniques used in past courses. The course needed to introduce business students to a range of topics that would be useful in a business setting. Where possible, we noted a list of options, such as in the course materials segment, to allow instructors to customize the course an undergraduate or graduate environment. Likewise, one could adapt the topics covered in our proposed course to vary between a graduate course (e.g., more focus on the governance activities of senior executives) and an undergraduate course (e.g., more technical fundamentals elements). We explain the course in more details in Section 4.

[3] We note that the non-business course sample includes a high proportion of course offerings from schools of computer science. This distribution appears to represent the departmental offerings of information security courses because, in our search approach, we did not distinguish on the basis of department. Although we could not locate additional syllabi from engineering, information science, law, and math, we noted unique and valuable elements from these courses that contributed to our findings. Future research could further investigate the nature of these less-common course offerings.

Table 1. Coding Categories[a]

Category	Subcategory	Number of syllabi corresponding with the subcategory[b]	Total passages coded[c]
Class objectives/ motivation	• Analysis skills regarding security issues	8	193
	• Conceptual or theoretical understanding of security	5	
	• Develop understanding of social, ethical, or legal aspects of security	21	
	• Managerial or organizational aspects of security	31	
	• Technical understanding of security issues	42	
	• Tool-specific, hands-on security skills	10	
Course materials	• Textbooks	41	68
	• Podcasts	1	
	• Supplementary readings (including case studies, journal readings, practitioner publications)	13	
Student evaluation techniques	• Case studies	6	170
	• Exams, tests, quizzes	37	
	• Group papers or projects	14	
	• Homework assignments	12	
	• Individual papers or projects	30	
	• Lab assignments	7	
	• Participation	16	
	• Web-based exercises	2	
Topic areas covered	• General topic discussion	30	111
	• Access control (technical)	5	
	• Telecommunications and network security (technical)	7	
	• Software development security (technical)	4	
	• Cryptography (technical)	7	
	• Security architecture and design (technical)	3	
	• Operations security (technical)	2	
	• Physical (environmental) security (technical)	2	
	• Information security governance and risk management (non-technical)	7	
	• Information security program development and management (non-technical)	1	
	• Information security incident management (including business continuity and disaster recovery planning) (non-technical)	5	
	• Legal, regulations, investigations and compliance (non-technical)	5	
	• Other topics (including computer forensics, privacy, intellectual property)	13	

[a] Refer to Appendix B for representative examples of each coding category.
[b] This column represents the number of information security syllabi (out of a total of 44) that contain at least one passage corresponding to the respective subcategory. Some syllabi have multiple passages coded to the same subcategory.
[c] This column represents the total number of passages, across all 44 syllabi, that correspond to a category.

4 Results

Drawing on observations from reviewing the 44 information security syllabi, we first detail the nature of the data and summarize the observations stemming from our analysis. Broadly speaking and as we expected, most computer science and engineering courses had a significant component that focused on the technical aspects of information security, including topics such as access control, network security, and software development security. We found that many courses emphasized cryptography and cryptographic algorithms. Similarly, security courses in business schools typically had a notable component that focused on organizational issues, risk management, and security policy topics. We noted similar patterns across both undergraduate and graduate courses.

However, despite each discipline's broad leanings towards technical or managerial content, we were generally surprised by the similarities in content across departments/colleges. Of the 44 syllabi reviewed, 42 included course objectives related to security's technical elements, while 31 noted objectives related to security's managerial aspects. In fact, many business classes appeared to delve into reasonably technical content on cryptography and network security. Likewise, many computer science and engineering courses (e.g., North Carolina AT&T, NYU Polytechnic, Pittsburgh State, Johns Hopkins, Marshall) covered aspects of security governance, risk management, and other organizationally focused aspects of security. In some cases, we found it difficult to discern which discipline offered the course based only on the content listed in the syllabus, which suggests that universities offering security classes from two or more departments may have wasted effort in creating similar material, particularly when offerings target students with a limited background in the subject. As Appendix A notes, the majority of courses were introductory courses and had titles including terms such as "introduction", "foundations", and "principles". The relative lack of advanced courses focusing on a particular topic, such as cryptography or network security, is somewhat surprising.

We also did not expect the relatively limited role of hands-on, tool-specific instruction noted in the syllabi. We identified only ten courses that included such a component, which suggests that the majority of security courses, even those technical in nature, may have limited opportunities for students to develop practical experience with the security tools they would use in future jobs. Although this method of training is consistent with the examination approach that many security certifications (e.g., CISSP) adopt, newly emerging credentials such as the CSX practitioner certification from ISACA require a performance-based examination of skills such as vulnerability assessment. As Andress (2014a) notes, one should distinguish formal security education, which we focus on in this study, from such non-university security training and credentials.

We were also surprised to find that only six courses used case studies. Noteworthy exceptions include SUNY Buffalo, Temple, Notre Dame (technology risk management course), and Bentley. Case studies are a staple of business courses in management, marketing, and organizational behavior, but past research has also highlighted their usefulness in information security education (He, Yuan, & Yang, 2013). Of those information security classes using case studies, we found little overlap in the materials used. Instructors are possibly using the short, end-of-chapter cases that some textbooks include, or they may not believe that one can use cases effectively in teaching security. However, we suggest that a general lack of published security-oriented case studies limits the choices available. We address this issue in more detail in Section 5.

We identified a total of 36 textbooks listed in the security syllabi as either required or optional. Of those, only seven texts were used at more than one school and only two texts were used at more than two schools (see Appendix C). Whitman & Mattord's *Management of Information Security* was the most popular text; it was required in seven courses and optional in two more courses. Andress' *The Basics of Information Security* was the next most popular; it was required at two schools and optional at a third. Additionally, some courses used textbooks associated with professional security designations (CISSP, CompTIA Security+, CAP). Interestingly, no courses adopted the official $(ISC)^2$ guide to the CISSP exam (perhaps due to its 1520 page length) or the official guide to the CAP exam. Books that the courses we reviewed didn't consider but may warrant consideration include the official $(ISC)^2$ guide to the information systems security management professional (ISSMP) and the CISM review manual from ISACA.

Further, we found that only five courses included any sort of explicit statement or agreement in the course syllabus to avoid hacking or other unethical, security-related activities (i.e., a white hat agreement). Exceptions included courses offered by UMass, University of Idaho, Boise State, Georgia Tech, and the University of Washington. Of those schools that did include an ethics section in their syllabi, many

required students to explicitly sign and agree to the guidelines. At least for the business school courses, instructors may not consider the depth of student skills or the tools covered in class to be sufficient to warrant such a formal statement. However, past research has highlighted the importance of instructors and institutions to clearly state the boundaries under which students should conduct their security-related learning (Xu, Hu, & Zhang, 2013). In a related point, we identified few assignments or projects that exposed students to security issues or techniques outside the classroom or laboratory. The most notable exception to this observation was at the University of Washington, where a group project required students to conduct a social engineering or war-walking exercise on campus. Past research has noted the potential benefits and the ethical risks inherent in "teaching students to hack" (Logan & Clarkson, 2005).

4.1 Teaching Information Security: Novel Techniques

While analyzing the information security syllabi, we noted a variety of novel, interesting, and useful approaches to teaching the subject. In some cases, we had used these techniques in their own teaching, but, in many cases, we had not. We discuss them below to inform other instructors and to act as a foundation for the proposed course that we outline below.

Six of the courses we reviewed provided either a collection of supplementary links to websites that discuss security-related topics (e.g., infosecurity-magazine.com) in their syllabus or an optional/supplementary reading list for students new to the discipline. Because information security may be a new topic for many students (particularly in business schools), this information highlighted sources of current events and related news in the discipline. Due to the range of backgrounds of business students, we see such an approach as a valuable technique to even the playing field among students new to the topic.

Another interesting approach that we noted was to have options embedded in the course design that enabled students to adjust the degree of technical versus managerial focus to their own interests and aptitudes. For example, the information security course at Rutgers identified three options for the individual research paper: a survey paper drawing on published research, a research paper on a new area of inquiry initiated by the student, or a prototype implementation. Such an approach can allow a wider range of students to develop skills in the areas of security that interest them rather than, for example, forcing a marketing major to develop a software prototype or an IT major to examine risk management principles. Hence, this approach can potentially address the issue of a single information security course's not being able to meet the needs of both technical and non-technical business students. Although we recognize the importance of pushing the limits of student knowledge, we argue that allowing some degree of flexibility in some of the course content can aid in developing student interest and knowledge.

We also noted that sixteen of the courses we reviewed included participation grades. Although we recognize that such grades can be an ambiguous and time-intensive method of evaluation, some syllabi we reviewed employed interesting techniques. For example, at Temple, 20 percent of the class grade was allocated to participation and comprised an element before class (briefly summarize each session's readings and post a link to a security article to the online discussion board), during class (discussion about readings), and between classes (reading and commenting on the class blog). This approach may allow for those students uncomfortable with speaking up in class to engage in alternative ways to contribute to the class discussions.

A few classes made explicit links in their syllabi to security-oriented professional designations (e.g., NYU Poly, Washington) and practitioner frameworks such as COBIT (e.g., UMass-Boston, Penn State, Eastern Michigan). As we note above, some courses even used certification-oriented textbooks. We argue that drawing clear links between the course content, employment opportunities, and practitioner-oriented tools/frameworks can help to provide context and incentives for students to recognize the practical, real-world applications of security in a business environment. To enhance these links, some courses (e.g., Pittsburgh State, Temple) required students to identify current security events throughout the semester. Although we expect that many instructors would raise current events in classroom discussion or on the class website, putting the responsibility for identifying such events on the students could further develop their interest and expertise in the discipline. Other courses used social media, such as Twitter, to share comments and security event news with students. For example, one syllabus specified that all students had to join the class-specific Twitter feed.

4.2 A Proposed Course Outline

We proceeded to synthesize the elements from each of the categories to create an introductory information security course that would best represent the key foundational technical and managerial content and draw on the novel pedagogical techniques described above. We created a course organized around two modules: technical foundations and managerial foundations. We wanted to align the class content to one or two textbooks and demonstrate a basic degree of consistency with one or more of the professional certifications that would be of interest to business students studying information security. Table 2 summarizes the results. Though we recognize that the proposed course may not be ideal for all schools, students, or instructors, we believe it provides an overall foundation of balanced technical and managerial perspectives and allows instructors to tailor it to their own unique circumstances.

Table 2. Outline of Proposed Information Security Course

Category	Hybrid course details
Class objectives/motivation	1. To provide a solid foundation of the technical and non-technical aspects of information security. 2. To develop analytical skills related to information security issues and challenges. 3. To establish an understanding of the social, ethical, and legal aspects of information security. 4. To introduce the core conceptual and theoretical models used in information-security research and practice. 5. To examine the key elements of organizational concerns related to information security. 6. To outline a variety of the key technical issues and tools used in information security.
Course materials	Andress (2014b) Whitman & Mattord (2013)
Student evaluation techniques	**Group project (20% of final grade):** working in small groups, students will select an information security software tool, install it in a campus computer lab (where permitted) or on their personal computer, and provide a demonstration to the class. A 10-page report describing the tool, its functionality, output, and an assessment of the organizational value/importance of the product should accompany the presentation. The instructor will assign students to teams to ensure a balance of technical and managerial skills. **Individual project (20% of final grade):** a 15-page research paper on a topic of the student's choice. A variety of technical (e.g., examining recent malware exploits) and managerial (e.g., managing security risks in the financial services industry) topics are permitted. **Participation (15% of final grade):** 5% will comprise students submitting a brief summary of each session's readings prior to class; 5% will comprise active participation in class discussions; 5% will comprise active participation on the class blog/discussion board (e.g., comments on current events, posting of security-related news stories, continuation of class discussions). **Midterm exam (15% of final grade):** comprises a mix of short answer and case study questions. **Final exam (30% of final grade):** comprises a mix of short answer and case study questions.
Topic areas covered	**Module 1: Technical foundations of information security** Week 1: Access control Week 2: Telecommunications and network security Week 3: Software development security Week 4: Cryptography Week 5: Security architecture and design Week 6: Operations security Week 7: Physical and environmental security **Module 2: Managerial foundations of information security** Week 8: Information security governance and policy Week 9: Information risk management and data security Week 10: Information security compliance and auditing Week 11: Information security program development, program management and project oversight Week 12: Information security incident management, business continuity and disaster recovery planning Week 13: Legal, regulations, standards and investigations Week 14: Information security ethics

Each element in the course outline draws on insights garnered from the syllabi review. The class objectives/motivation section builds on 193 objectives extracted from the collected syllabi. We synthesized the six items listed from the coded passages, and the items represent a balance of both technical and managerial content. Similarly, we developed the evaluation techniques based on reviewing 170 elements that we coded from the collected data. Although one could adopt numerous approaches to evaluate students, our proposed approach includes elements that integrate both technical and managerial content. For example, the group project specifies both technical and managerial elements. However, the individual project allows students the flexibility to focus on a topic of interest regardless of the technical/managerial content.

We generated the topic areas based on 111 passages that we coded from the collected syllabi. We sorted the key patterns that emerged into groupings focusing on technical and managerial foundations. Based on the topic areas we identified, we compared the coverage in the two most popular textbooks and two popular security certifications (one technically-oriented: CISSP; the other managerially-oriented: CISM). Table 3 highlights this balance. Although we reviewed the content in other textbooks, we found the two selected for this proposed class to be highly effective in addressing the content without overlapping in any significant areas. One would expect each of these topic areas to address not only the technical elements of a topic area (e.g., the design of an authentication mechanism for an application) but also the behavioral elements of security (e.g., the challenges that employees have in creating and remembering strong passwords).

Table 3. Topic Mapping to CBK and Textbooks

Topic areas	Textbook mappings		Certification mappings	
	Whitman & Mattord (2013)	Andress (2014b)	CISSP	CISM
Access control		x	x	
Telecommunications and network security		x	x	
Software development security		x	x	
Cryptography		x	x	
Security architecture and design		x	x	
Operations security		x	x	
Physical and environmental security		x	x	
Information security governance	x		x	x
Information risk management	x		x	x
Information security compliance and auditing	x		x	x
Information security program development and management	x		x	x
Incident management, business continuity, disaster recovery	x		x	x
Legal, regulations, and investigations	x		x	
Information security ethics	x			

5 Discussion

In this paper, we review the current pedagogical practices of information security instructors that an introductory business school course could also employ. We drew on information security syllabi across a range of disciplines to identify novel approaches that could aid in balancing the delivery of both managerial and technical content to students.

As we note above, the proposed course outline may not be suitable for all business school-based information security courses, but we believe it provides a solid foundation from which instructors can make customizations to suit their needs. Such adjustments could include adding or removing topic areas depending on other courses being offered and guest lectures or co-taught portions of the course with

instructors from computer science, engineering, and/or law (depending on the topic). During our analysis, we reviewed several courses that supplemented traditional security topics with other areas such as computer forensics, privacy, and intellectual property. Adding such topics could aid in meeting the needs of students and in leveraging the instructor's expertise.

5.1 The Future of Information Security in Business Schools

The demand for graduates with skills in information security, the quickly changing nature of the discipline, and the political complexity of offering similar courses alongside other departments/colleges in a university makes information security an important topic to address (Woodward et al., 2013). Fundamental to this discussion is clearly establishing the role that business schools play in delivering information security education to students. Based on the rich history of security in other disciplines, it seems that computer science and engineering best deliver security's purely technical aspects just as law departments best deliver the legal aspects. However, we argue that business schools are well positioned to address security's risk management, control, and policy-related elements. Further, by having a distinctly organizational perspective on the topic, business schools are uniquely positioned to apply technical security concepts into the context of business. Although business students stand to gain by developing technical security skills and knowledge sought by employers, non-business students also stand to gain by supplementing the security knowledge developed in other classes with a distinctly business perspective.

To that end, we see a notable opportunity for interdisciplinary *collaboration* on information security courses. Larger schools or those with expanded information security course offerings could offer a collection of complementary courses that faculty from various departments (e.g., computer science, business, and law) could teach or co-teach. Such courses could include specialized classes focusing on security governance or security risk management to supplement the introductory content in a course such as the one we have outlined.

However, to enable such a step forward, the academy and those employers who hire business school graduates need to better communicate with each other, which may entail a renewed effort to clarify exactly what knowledge and skills employers desire in new hires. Moreover, improved communication between business schools and other departments that run security courses is of critical importance. These courses need to align to limit overlap and provide students with the knowledge they need as they join the workforce. We acknowledge the political challenges inherent in facilitating courses across departments/colleges. In situations where security courses have been controlled by a single department for an extended period and where funds are allocated to departments based on the number or courses or enrolled students, introducing such hybrid courses may be particularly difficult.

Additionally, as we note above, the materials that information-security classes rely on differ widely. Though one may expect such a finding due to the variety of textbooks available on the market, we see a distinct opportunity to develop and publish more security-oriented case studies. We encourage authors to write, publish, and communicate the availability of security cases for classroom use.

6 Conclusion

In this paper, we address the unique aspects of teaching information security in a business school, what pedagogical challenges exist for instructors, and what measures faculty can take to address these challenges. We build on past pedagogical research on information security (e.g., Jensen & Cline, 2005; Walter, 2007; Yurcik & Doss, 2001) and found that many instructors have employed novel techniques to educate students on information security-related issues and topics. However, we found overlap between the content being covered in business and non-business courses. To this end, we outline and discuss a hybrid approach to teaching information security in business schools that incorporates a range of technical and managerial topics. We see this approach as a means to at least partially address the pedagogical challenges inherent in teaching this subject the needs of an increasingly diverse population of business students that includes both technical and non-technical backgrounds.

Our study has several limitations. First, we used publicly available syllabi posted online as our data. Hence, this sample may not represent all information security courses. Second, and related to the previous point, the syllabi came from only schools in the US; it is possible that information security courses are taught differently in other areas of the world. Third, the course syllabi contained varying levels of detail and addressed different elements of information security education. To achieve an inclusive view of the discipline, we weighted each syllabus equally. Those students or schools with a decidedly technical

versus managerial view of security may consider some syllabi to be of relatively greater importance. Finally, our proposed hybrid course may not be appropriate for a school with extensive information security course offerings but rather for a school that currently offers only one or two information security courses.

In moving this line of inquiry forward, future work can extend and enhance our research by surveying faculty teaching information security to collect their insights on the pedagogical challenges and opportunities for the discipline. By expanding the scope of such a review to both non-U.S. schools and schools with syllabi not posted currently online, researchers may uncover additional opportunities to identify patterns and unique pedagogical practices in security courses. Likewise, focusing on the broader characteristics of degree programs that specialize in security (rather than on the characteristics of the security courses themselves) may further explain the technical and managerial variability in security course offerings. Finally, future studies could examine the particular skills that the job market demands and evaluate the extent that current course designs fulfill that need. Although this study represents an initial step in continuing to develop and refine security-oriented curriculum in business schools, future studies may also seek to identify improvements that instructors could make to more advanced security classes such as information security governance or information security incident management.

References

Andress, J. (2014a). Building information security professionals. *ISACA Journal*, *1*, 1-5.

Andress, J. (2014b). *The basics of information security* (2nd ed.). Waltham, Massachusetts: Elsevier.

Bishop, M. (2006). Teaching context in information security. *ACM Journal of Educational Resources in Computing, 6*(3), 1-12.

Bradshaw, D. (2015). Student and corporate demands shape curriculum. *Financial Times.* Retrieved from http://www.ft.com/cms/s/2/787a02aa-83cd-11e5-8095-ed1a37d1e096.html#axzz43LhDOyRQ

Cisco. (2014). *Cisco 2014 annual security report*. San Jose, California.

Denning, P. J., Parker, D. B., Nycum, S. H., & Ware, W. H. (1984). Computers, crime, and privacy—a national dilemma. *Communications of the ACM*, *27*(4), 312-321.

Foltz, C. B., & Renwick, J. S. (2011). Information systems security and computer crime in the IS curriculum: A detailed examination. *Journal of Education for Business, 86*, 119-125.

He, W., Yuan, X., & Yang, L. (2013). Supporting case-based learning in information security with Web-based technology. *Journal of Information Systems Education, 24*(1), 31-40.

Hernandez, S. (2012). *Official (ISC)^2 Guide to the CISSP CBK* (3rd ed.). Boca Raton, Florida: (ISC)^2 Press.

Hulme, G. V. (2012). *Unrealistic expectations, skills gap mire market for security jobs*. Retrieved from http://searchsecurity.techtarget.com/news/2240173143/Unrealistic-expectations-skills-gap-mire-market-for-IT-security-jobs

Hutchinson, W., & Warren, M. (2002). Developing a postgraduate course in information security: A confusion of terms. In *Proceedings of Australasian Conference on Information Systems*.

ISACA. (2014). *CISM review manual 2015*, Rolling Meadows, Illinois.

ISC^2. (2013). *The 2013 ISC^2 global information security workforce study*. Mountain View, CA.

Jensen, B. K., & Cline, M. (2005). Teaching information security courses: Objectives, requirements, and challenges. In *Proceedings of the Americas Conference on Information Systems.*

Landwehr, C. E. (2001). Computer Security. *International Journal of Information Security, 1*(1), 3-13.

Long, J., & White, G. (2010). On the global knowledge components in an information security curriculum—a multidisciplinary perspective. *Education and Information Technologies, 15*, 317-321.

Logan, P. Y., & Clarkson, A. (2005). *Teaching students to hack: Curriculum issues in information security*. St. Louis, Missouri: SIGCSE.

Miles, M. B., & Huberman, M. A. (1994). *Qualitative data analysis: An expanded source book*. Thousand Oaks, CA: Sage.

Morgan, S. (2015). Money talks: Send your kid to cybersecurity school. *CSO.* Retrieved from http://www.csoonline.com/article/2947484/it-careers/send-your-kid-to-cybersecurity-school.html

Ponemon Institute. (2013). *2013 cost of data breach study: Global analysis*. Traverse City, Michigan: Ponemon Institute Research Report.

SANS Institute. (2014). *Cybersecurity professional trends: A SANS survey*. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/cybersecurity-professional-trends-survey-34615

Walters, L. M. (2007). A draft of an information systems security and control course. *Journal of Information Systems*, *21*(1), 123-148.

White, G. L., Hewitt, B., & Kruck, S. E. (2013). Incorporating global information security and assurance in IS education. *Journal of Information Systems Education, 24*(1), 11-16.

Whitman, M. E., & Mattord, H. J. (2013). *Management of information security* (4th ed.). Stamford, Connecticut: Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2004). *Designing and teaching information security curriculum*. Kennesaw, Georgia: InfoSecCD Conference.

Woodward, B., Imboden, T., & Martin, N. L. (2013). An undergraduate information security program: More than a curriculum. *Journal of Information Systems Education*, *24*(1), 63-70.

Yurcik, W., & Doss, D. (2001). Different approaches in the teaching of information systems security. In *Proceedings of the Information Systems Education Conference*.

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become hackers. *Communications of the ACM*, 56(4), 64-74.

Appendix A: Information Security Syllabi Listing

Table A1. Information Security Syllabi Listing

School name	Course name	Discipline
Rutgers University	Information Security	Business
Georgia State University	Introduction to Security and Privacy of Information and Information Systems	Business
Dakota State University	Principles of Information Assurance	Business
Howard University	Information Assurance	Business
Howard University	Information Security	Business
Carnegie Mellon University	Introduction to Information Security Management	Business
Norwich University	Introduction to Information Assurance	Business
Norwich University	Management of Information Assurance	Business
University of Wisconsin-Eau Claire	Information Assurance	Business
Florida Atlantic University	Information Systems Security	Business
Florida Atlantic University	Security Management	Business
University of North Carolina at Greensboro	Information Systems Security	Business
Boise State University	Information Security	Business
University at Albany, SUNY	Information Security Policies	Business
SUNY Buffalo	Information Assurance	Business
University of Notre Dame	Technology Risk Management	Business
University of Notre Dame	Networking & Security	Business
Temple University	Protecting Information Assets	Business
New York Institute of Technology	Computer Information Systems Security	Business
Bentley University	Information Security and Computer Forensics	Business
Carnegie Mellon University	Applied Information Assurance	Computer science
North Carolina AT&T State University	Security Management for Information Systems	Computer science
San Jose State University	Information Security	Computer science
University of Idaho	Introduction to Information Assurance	Computer science
University of Texas – Dallas	Information Security	Computer science
New York University Polytechnic	Information Systems Security Engineering and Management	Computer science
College of Charleston	Information Security Principles	Computer science
Pittsburgh State University	Information Assurance and Computer Security I	Computer science
Pittsburgh State University	Information Assurance and Computer Security II	Computer science
University of Massachusetts-Boston	Introduction to Information Security	Computer science
St. John's University	Introduction to Information Security	Computer science
Georgia Tech University	Introduction to Information Security	Computer science
Mercy College	Topics in Information Security	Computer science
Athens Technical College	Information Security Fundamentals	Computer science
Purdue University	Information Security	Computer science
Johns Hopkins University	Foundations of Information Assurance	Engineering

Table A1. Information Security Syllabi Listing

Stevens Institute of Technology	Information Systems Security	Engineering
Southern Polytechnic State University	Introduction to Information Security	Engineering
Marshall University	Information Security	Engineering
University of Washington	Foundations of Organizational Information Assurance	Information science
Syracuse University	Introduction to Information Security	Information science
Pennsylvania State University	Information Security and Assurance	Information science
Eastern Michigan University	Legal Issues in Information Assurance/Security	Law
Florida Atlantic University	Cryptography and Information Security	Math
Rutgers University	Information Security	Business
Georgia State University	Introduction to Security and Privacy of Information and Information Systems	Business

Appendix B: Representative Examples of Coded Data

Table B1. Representative Examples of Coding Category Data

Category	Subcategory	Representative example
Class objectives/ motivation	Analysis skills regarding security issues	*Develop a "security mindset": learn how to critically analyze situations of computer and network usage from a security perspective, identifying the salient issues, viewpoints, and trade-offs.* (Georgia Tech University)
	Conceptual or theoretical understanding of security	*This course has been designed to integrate theoretical concepts with their practical applications so as to teach both the theory and the practice of information assurance.* (SUNY Buffalo)
	Develop understanding of social, ethical, or legal aspects of security	*A comprehensive, in depth study of the legal and ethical issues in computer security, as well as privacy laws and issues and strategies available to an enterprise is provided in this course.* (Howard University)
	Managerial or organizational aspects of security	*Define and understand the scope of the security problem in today's business environment.* (Boise State University)
	Technical understanding of security issues	*To enable students to understand security technologies such as cryptography, authentication, authorization, non-repudiation, and commercially available security packages (PKI, PGP, Kerberos, SSL, VPN).* (New York Institute of Technology)
	Tool-specific, hands-on security skills	*A few practical and hands-on approaches will be discussed to better explore networking security software and hardware tools.* (Florida Atlantic University)
Course materials Student evaluation techniques	Textbooks	*Computer and Information Security Handbook, John R. Vacca, Morgan Kaufmann 2008.* (Temple University)
	Podcasts	*Podcasts will be available in iTunesU in lieu of a full in-class chapter/topic lecture. Please review podcasts and complete related quizzes before class to stay current with course materials.* (Boise State University)
	Supplementary readings (including case studies, journal readings, practitioner publications)	*Suggested Readings Regularly visit the site: www.rsa.com, http://www.networkworld.com/topics/security.html.* (Howard University)
	Case studies	*Case Study Analyses: You will officially prepare two case studies that I assign you during the semester. For each case study I will provide several discussion questions. Pick one question and respond to it in depth.* (Temple University)
	Exams, tests, quizzes	*Exams/quizzes measure your understanding of key security concepts, issues, technologies, and terms. They will be a combination of multiple-choice, short answer, and short essay covering both business and technical fundamentals of information security. Exams will be given on our lab PCs during scheduled class time, with quizzes typically on Blackboard™ as shown in the schedule. Quizzes support the "assurance of learning" methodology & will combine individual & group quiz activities.* (Boise State University)
	Group papers or projects	*Group Project. There will be one or two group projects given during the semester. This is basically a research project, which combines technical knowledge with managerial skills. There will be group deliverables such as a project report and a presentation that you have to work on as a team. You have to work as a strongly coupled team, where you will actually be making a contribution to the state of practice in the information technology security arena.* (Florida Atlantic University)
	Homework assignments	*Homework: there will be two homework assignments, plus 2 blog posts that count together as a third homework. Homework assignments will be made available on Blackboard prior to the due date and homework submission will also take place in Blackboard.* (Carnegie Mellon)

Table B1. Representative Examples of Coding Category Data

	Individual papers or projects	*Term project: 20% of final grade: Students will write a 3,500 ± 500 word research paper on a suitable topic to be selected in conjunction with the instructor. Post your topic suggestion in the public discussion group on NUoodle 2. Instructor approval helps to avoid the problem of discovering that you have picked a topic worthy of a textbook and also prevents duplicate topics.* (Norwich University)
	Lab assignments	*During the course of semester, you will be given 7 lab assignments. The main objective of the labs is to give you hand on experience in using some of the tools used in Information Assurance. As you will see, the tools developed with the intent of aiding in maintenance and troubleshooting tasks can be used by hackers for the negative purposes. For example tool such as NMap which is used often by network administrators to see which servers (/services) are up and running can be used by hackers to see which ports are open to carry out the malicious activity.* (SUNY Buffalo)
	Participation	*Much of your learning will occur as you prepare for and participate in discussions about the course material. The assignments, cases, and readings have has been carefully chosen to bring the real world into class discussion while also illustrating fundamental concepts.* *To encourage participation, 20% of the course grade is earned by preparing before class and discussing the topics between and in class.* (Temple University)
	Web-based exercises	*A weekly blog will help you stay on top of current news and security issues and share your findings.* (Boise State University)
Topic areas covered	General topic discussion	*This course will examine security topics through the use and exploration of the "body of knowledge" as described in the Certified Information Systems Security Professional (CISSP) certification.* (Dakota State University)
	Access control (technical)	*Security basics: authentication, access control, and audit.* (Purdue University)
	Telecommunications and network security (technical)	*Networks: wired and wireless networks, protocols, attacks and countermeasures.* (Georgia Tech University)
	Software development security (technical)	*Software security: vulnerabilities and protections, malware, program analysis.* (Georgia Tech University)
	Cryptography (technical)	*Identify cryptography and encryption-based solutions* (Athens Technical College)
	Security architecture and design (technical)	*Performing vulnerability assessments*. (Florida Atlantic University)
	Operations security (technical)	*Develop, analyze, and implement security policies and best practices to achieve CIA (confidentiality, integrity, and availability).* (Boise State University)
	Physical (environmental) security (technical)	*Identify key physical threats to the information facility* (Athens Technical College)
	Information security governance and risk management (non-technical)	*Develop processes for system evaluation and assurance and understand what frameworks are commonly used for governance and compliance activities.* (Carnegie Mellon University)
	Information security program development and management (non-technical)	*Developing the security program.* (Florida Atlantic University)
	Information security incident management (including business continuity and disaster recovery planning) (non-technical)	*Understand what is required to formulate and implement a plan for incident response.* (Carnegie Mellon University)

Table B1. Representative Examples of Coding Category Data

	Legal, regulations, investigations and compliance (non-technical)	*Identify the legal, ethical, and profession issues in information security: List laws relevant to information security; Identify international laws and legal bodies.* (Athens Technical College)
	Other topics (including computer forensics, privacy, intellectual property)	*Explain the basic concept and importance of intellectual property law and legal ownership.* (Eastern Michigan University)

Appendix C: Information Security Textbook Listing

Table C1. Information Security Textbook Listing

Text	Location of textbook adoptions
Andress, J. (2014b). *The basics of information security* (2nd ed.). Waltham, Massachusetts: Elsevier.	Bentley, Boise State, Southern Poly
Bosworth, S., Kabay, M. E., & Whyne, E. (2009). *Computer security handbook* (5th ed.). Hoboken, New Jersey: Wiley.	Norwich, University of Wisconsin-Eau Claire
Ciampa, M. (2011). *Security+ guide to networking security fundamentals (3rd ed.).* Boston, Massachusetts: Cengage Learning.	Florida Atlantic, Athens Technical College
Panko, R. (2010). *Corporate computer and network security* (2nd ed.). Boston, MA: Prentice Hall.	Notre Dame, Pittsburgh State
Pfleeger, C. P. (2006). *Security in computing (4th ed.).* Lawrence, IL: Prentice Hall.	Howard University, University of Idaho
Stewart, J., Chapple, M., & Gibson, D. (2012). *CISSP: Certified information systems security professional study guide (6th ed.).* Indianapolis, IN: Sybex.	Dakota State University, Penn State
Whitman, M. E., & Mattord, H. J. (2013). *Management of information security (4th ed.)*. Stamford, Connecticut: Cengage Learning.	Florida Atlantic, NYIT, SUNY Buffalo, Notre Dame, North Carolina AT&T, NYU Poly, St. John's University, UMass-Boston, Marshall

About the Authors

W. Alec Cram is an Assistant Professor of Information and Process Management at Bentley University. He received his PhD from Queen's University. Before returning to school, Alec worked as an IT Audit Manager at Deloitte, where he received a CISSP and CISA. Alec currently teaches undergraduate and graduate information security classes. His research focuses on how information systems control initiatives can contribute to improving the performance of organizational processes. His work has been published or is forthcoming in outlets including the *Information Systems Journal*, *European Journal of Information Systems*, *Journal of the Association for Information Systems,* and *Information & Management*.

John D'Arcy is an Associate Professor in the Department of Accounting & MIS, Lerner College of Business and Economics, at the University of Delaware. He received his PhD in Management Information Systems from Temple University. His research interests include information assurance and security, IT risk management, and computer ethics. His work appears in journals such as *Information Systems Research*, *Decision Sciences Journal*, *European Journal of Information Systems*, *Journal of Management Information Systems*, *MIT Sloan Management Review*, *Decision Support Systems*, and *Computers & Security*.