In this issue:

4. **Certifying Business Students in Microsoft Office Specialist Certification Excel Core Exam: Lessons Learned**  
Nesrin Bakir, West Texas A&M University  
Kareem Dana, West Texas A&M University  
Amjad Abdullat, West Texas A&M University

12. **Intellectual Merit and Broader Impact: Collaborative Education toward Building a Skilled Software Verification and Validation Community**  
Sushil Acharya, Robert Morris University  
Priyadarshan A. Manohar, Robert Morris University  
Peter Y. Wu, Robert Morris University

22. **Data Cleansing: An Omission from Data Analytics Coursework**  
Johnny Snyder, Colorado Mesa University

30. **Process-Focused Approach to a Systems Analysis & Design Group Project**  
Aditi Mukherjee, University of Florida  
Sarah Bleakney, University of Florida

41. **Dotting i’s and Crossing T’s: Integrating Breadth and Depth in an Undergraduate Cybersecurity Course**  
David J. Yates, Bentley University  
Mark Frydenberg, Bentley University  
Leslie J. Waguespack, Bentley University  
Isabelle McDermott, Bentley University  
Jake O’Connell, Bentley University  
Frankie Chen, Bentley University  
Jeffry S. Babb, West Texas A&M University
The Information Systems Education Journal (ISEDJ) is a double-blind peer-reviewed academic journal published by ISCAP (Information Systems and Computing Academic Professionals). Publishing frequency is six times per year. The first year of publication was 2003.

ISEDJ is published online (http://isedj.org). Our sister publication, the Proceedings of EDSIGCON (http://www.edsigcon.org) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the EDSIGCON conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the ISEDJ journal. Currently the target acceptance rate for the journal is under 40%.

Information Systems Education Journal is pleased to be listed in the Cabell's Directory of Publishing Opportunities in Educational Technology and Library Science, in both the electronic and printed editions. Questions should be addressed to the editor at editor@isedj.org or the publisher at publisher@isedj.org. Special thanks to members of AITP-EDSIG who perform the editorial and review processes for ISEDJ.

2019 Education Special Interest Group (EDSIG) Board of Directors

<table>
<thead>
<tr>
<th>President</th>
<th>Vice President</th>
<th>Past President</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jeffry Babb</td>
<td>Eric Breimer</td>
<td>Leslie J Waguespack Jr.</td>
</tr>
<tr>
<td>West Texas A&amp;M</td>
<td>Siena College</td>
<td>Bentley University</td>
</tr>
<tr>
<td>President</td>
<td></td>
<td>Past President</td>
</tr>
<tr>
<td>Amjad Abdullat</td>
<td>Lisa Kovalchick</td>
<td>Niki Kunene</td>
</tr>
<tr>
<td>West Texas A&amp;M</td>
<td>California Univ of PA</td>
<td>Eastern Connecticut St Univ</td>
</tr>
<tr>
<td>Director</td>
<td>Director</td>
<td>Director</td>
</tr>
<tr>
<td>Li-Jen Lester</td>
<td>Lionel Mew</td>
<td>Rachida Parks</td>
</tr>
<tr>
<td>Sam Houston State University</td>
<td>University of Richmond</td>
<td>Quinnipiac University</td>
</tr>
<tr>
<td>Director</td>
<td>Director</td>
<td>Director</td>
</tr>
<tr>
<td>Jason Sharp</td>
<td>Michael Smith</td>
<td>Lee Freeman</td>
</tr>
<tr>
<td>Tarleton State University</td>
<td>Georgia Institute of Technology</td>
<td>Univ. of Michigan - Dearborn</td>
</tr>
<tr>
<td>Director</td>
<td>Director</td>
<td>JISE Editor</td>
</tr>
</tbody>
</table>

Copyright © 2019 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to Jeffry Babb, Editor, editor@isedj.org.
INFORMATION SYSTEMS EDUCATION JOURNAL

Editors

Jeffry Babb
Senior Editor
West Texas A&M University

Anthony Serapiglia
Teaching Cases Co-Editor
St. Vincent College

Muhammed Miah
Associate Editor
Tennessee State University

Thomas Janicki
Publisher
U of North Carolina Wilmington

Paul Witman
Teaching Cases Co-Editor
California Lutheran University

James Pomykalski
Associate Editor
Susquehanna University

Donald Colton
Emeritus Editor
Brigham Young Univ.
Hawaii

Guido Lang
Associate Editor
Quinnipiac University

Jason Sharp
Associate Editor
Tarleton State University

2019 ISEDJ Editorial Board

Samuel Abraham
Siena Heights University

Joni Adkins
Northwest Missouri St Univ

Wendy Ceccucci
Quinnipiac University

Ulku Clark
U of North Carolina Wilmington

Amy Connolly
James Madison University

Jeffrey Cummings
U of North Carolina Wilmington

Christopher Davis
U of South Florida St Petersburg

Gerald DeHondt II
Ball State University

Catherine Dwyer
Pace University

Mark Frydenberg
Bentley University

Biswaip Ghosh
Metropolitan State U of Denver

Audrey Griffin
Chowan University

Janet Helwig
Dominican University

Melinda Korzaan
Middle Tennessee St Univ

James Lawler
Pace University

Paul Leidig
Grand Valley State University

Li-Jen Lester
Sam Houston State University

Michelle Louch
Duquesne University

Richard McCarthy
Quinnipiac University

Alan Peslak
Penn State University

Doncho Petkov
Eastern Connecticut State Univ

RJ Podeschi
Millikin University

Franklyn Prescod
Ryerson University

Bruce Saulnier
Quinnipiac University

Dana Schwieger
Southeast Missouri St Univ

Karthikeyan Umapathy
University of North Florida

Leslie Waguespack
Bentley University

Charles Woratschek
Robert Morris University

Peter Y. Wu
Robert Morris University

©2019 ISCAP (Information Systems and Computing Academic Professionals)
Dotting i’s and Crossing T’s: Integrating Breadth and Depth in an Undergraduate Cybersecurity Course

David J. Yates
dyates@bentley.edu

Mark Frydenberg
mfrydenberg@bentley.edu

Leslie J. Waguespack
lwaguespack@bentley.edu

Isabelle McDermott
mcdermo_isab@bentley.edu

Jake OConnell
oconnel_jake@bentley.edu

Frankie Chen
chen_fran@bentley.edu

Computer Information Systems Department
Bentley University
Waltham, MA

Jeffry S. Babb
jbabb@wtamu.edu

Computer Information and Decision Management Department
West Texas A&M University
Canyon, TX

Abstract

The importance of updating, expanding and improving what is taught in cybersecurity curricula is increasing as the security threat landscape becomes more dangerous, breaches become more frequent, and the number of deployed Internet of Things (IoT) devices, known for their security challenges, grows exponentially. This paper argues that a profile of “T-shaped” skills, which is known to be desirable in many consulting and design professions, is being reflected in the latest manifestations of cybersecurity curriculum design and accreditation. A model of learning that yields “T-shaped” professionals combines the ability to apply knowledge across domains (breadth) with the ability to apply functional and disciplinary skills (depth). We present the design of a junior- or senior-level cybersecurity course in which the horizontal stroke of the “T” (representing breadth) spans knowledge areas that cut across the people, process and technology triad. The vertical stroke of the “T” (representing depth) is provided by two aspects of the course design: first, learning the foundational principles of cybersecurity, including practical examples from cryptography and network security; and second, applying the principles of cybersecurity to a semester project, allowing students to expand the core “T” of the course to satisfy their own passions and interests. Our paper concludes with student and instructor reflections on the implementation of this cybersecurity course, as well as broader implications of the lessons learned after the initial offering of this course.
Keywords: Cybersecurity curricula, cybersecurity education, knowledge areas, security accreditation, cybersecurity course design, T-shaped knowledge and skills, security certification.

1. INTRODUCTION

Cybersecurity as a field of study began as soon as computers transitioned from stand-alone devices to being connected directly to a network, or to another device that is connected to a network. Thus, what we know today as cybersecurity began at the intersection of computer security (Bishop, 2018) and network security (Stallings, 2017). As computing and networks have become pervasive, security concerns have expanded to include application security, database security, infrastructure security, cloud, web and mobile security, and similar topics. Today information security and cybersecurity are two distinct, but related, umbrella disciplines that reflect the union of many areas of security.

Information security is defined in Andress (2014) as “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction’ according to U.S. law.” [p. 3]

Cybersecurity (sometimes written as Cyber security) is defined in Burley & Bishop et al. (2017) as a “computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management.” [p. 16]

These definitions suggest that security (in the large) is inclusive of many areas that are broad in their own right, e.g., computing, engineering, communication, human factors, law, ethics, policy, psychology, sociology, management, and even economics (Anderson, 2001). Hence attempts to disentangle one area within cybersecurity from another is like trying to separate and transplant one part of a Banyan Tree from another (see Figure 1).

The analysis, insights and reflections in this paper are, in part, a call to action to college and universities to develop and deliver the knowledge and skills that are needed to prepare their graduates for one of the many possible careers that fall under the cybersecurity umbrella (Newhouse, Keith, Scribner, & Witte, 2017; NIST, 2018; NSA, 2018a; Singer & Friedman, 2014).

Figure 1. Banyan Tree photographed on Oahu, Hawaii

This study focuses on the design and implementation of an undergraduate cybersecurity course based on the Burley and Bishop et al. (2017) definition presented above. In describing and illustrating this design, and also considering implications for accreditation and certification, we observe that a profile of knowledge and skills that yields “T-shaped people” (Guest, 1991; Brown, 2009; Sandeen & Hutchinson, 2010) is being reflected in the latest recommendations for cybersecurity education in academia as well in practice.

2. T-SHAPED KNOWLEDGE AND SKILLS

In our application of a T-shaped model of knowledge and skills (Madhavan & Grover, 1998; Peters, 2012) to cybersecurity, the horizontal bar of the “T” represents breadth and spans knowledge areas that cut across the people, process and technology triad (Andress, 2004). The vertical bar of the “T” represents depth and is based on the foundational principles of cybersecurity based in computing disciplines (Parekh & DeLatte, 2018). Furthermore, these foundational principles are strengthened by pairing them with practical examples from cryptography (Stallings, 2017), computer security (Bishop, 2018) and network security (Kaufman, Perlman, & Speciner, 2002).

The next section of the paper describes the T-based model for our cybersecurity course design and relates the course content to the latest curricula guidelines (Burley & Bishop, 2017). These guidelines reflect a two-year collaboration among the ACM, IEEE (CS), AIS (SIGSEC) and
IFIP. We then describe how students taking the course augmented the knowledge and skills embedded in the core "T" of the course with depth in specific areas developed as part of a course project. We conclude with an analysis of the current state of cybersecurity accreditation, reflections on the student and instructor experiences of the course, and finally offer our thoughts on improving or adapting the course at the center of this study in different ways.

3. COURSE DESIGN AND IMPLEMENTATION

Both cybersecurity and information security are multidisciplinary fields of study. Table 1 (see below) and Appendix A make this case for cybersecurity, which includes concepts as diverse as security design principles, digital forensics, identity management, and cyber ethics, among many others. Likewise, Crowley (2003) summarizes more than 24 important content areas included in U.S. government and commercial efforts to provide educational guidance to professionals working in, or students aspiring to work in, information security. Not surprisingly, factoring just one course from the eight cybersecurity Knowledge Areas (KAs) shown in Table 1 was challenging. The solution to this challenge required an integrated design (Iansiti, 1995) connecting the breadth of the course (the holistic, multidisciplinary horizontal bar in Figure 2) to the depth of the course (the technical vertical bar in Figure 2) and vice-versa.

Note that the KAs in Table 1 are listed in order from the lowest level (i.e., data and software security) to the highest level (i.e., organizational and societal security).

![Table 1. Knowledge Areas (KAs) in 2017 ACM, IEEE (CS), etc. JTF Undergraduate Curriculum Guidelines, aka (Burley & Bishop, 2017)](table1.png)

The horizontal stroke of the "T" in Figure 2 includes people, process and technology concerns (Andress, 2004). The vertical stroke is dominated by technology concerns. Brown (2009) would describe a person with fluency in relating and connecting areas on the horizontal in Figure 2 as an integrative thinker and skilled generalist and a person with fluency in all areas on the vertical as a deep thinker and skilled specialist (a so-called "i"). An ideal person (e.g., employee, consultant or designer) in most socio-technical realms has T-shaped knowledge and skills that enable her to think adaptively and to move seamlessly between being a skilled generalist and a skilled specialist (Brown, 2009).

![Figure 2. Cybersecurity Knowledge Areas organized in a "T" reflecting holistic, multidisciplinary breadth and technical depth](figure2.png)

The cybersecurity course offered at Bentley University was intended to teach students cybersecurity principles and practices, favoring technical content over non-technical content. Using the disciplinary lenses summarized in Burley and Bishop et al. (2017), the syllabus presented in Appendix B reflects the mostly technical computing disciplines in the approximate percentages shown in Figure 3. Although Figure 2 is our own creation, the graphic component of Figure 3 – showing interdisciplinary content from at least five domains plus five computing disciplines – is recreated from Figure 2 in Burley & Bishop et al. (2017).

In an "i-shaped" course design, students develop deep skills and experience in one area but may not apply or connect those skills to other areas or disciplines. Although the percentages in Figure 3 might suggest an "i-shaped" cybersecurity course design, the textbook for the course selectively presented people and process as well as technical...
concerns. The technical areas we covered in eleven chapters in Stallings (2017) were mostly grounded in discrete mathematics, computer science and computer engineering.

![Diagram showing Interdisciplinary Content]

Figure 3. Disciplinary lens for Bentley University CS 401 cybersecurity course

The CS 401 course offered at Bentley University transitioned from textbook readings to supplemental readings in Week 12. Two of the five supplemental readings were grounded in information systems and information technology (NIST, 2018; US DHS, 2016). The other three supplemental readings (Bonneau & Miller, 2015; Chen, Paxson, & Katz, 2010; Nakamoto, 2008) were grounded in computer science and software engineering. Taken together these six resources yielded the T-shaped course implementation shown in Figure 4. Note that Figure 4 duplicates the Knowledge Areas cast as a "T" in Figure 2, but adds the week-by-week coverage (listed as red numbers ranging from 1 to 14) shown in the course syllabus from the Spring 2018 rendition of CS 401.

![Diagram showing Cybersecurity]

Figure 4: Bentley University CS 401 cybersecurity course “T” implementation annotated with week-by-week coverage detailed in Appendix B

The CS 401 course was offered as a directed study for three conscientious students, all of whom are Computer Information Systems majors, during their junior or senior year at Bentley University. U.S. News and World Report ranked Bentley University highly as an internationally recognized business university with "more selective" admission standards in 2018. The syllabus presented in Appendix B, including the selection of textbook and readings, is therefore designed for above average (or stronger) undergraduate students. This means that although the cybersecurity course design reflected in Table 1 and Figure 2 is easily portable to other technical-focused curricula, the implementation reflected in Figure 3 and Figure 4 may or may not be.

We now turn our attention to the three cybersecurity course projects that counted for 45% of each student’s grade in CS 401. Although these projects were developed and submitted in phases as individual projects, similar team course projects -- adapted to local pedagogical norms -- could be developed for larger class sizes.

4. BENTLEY UNIVERSITY CS 401 STUDENT PROJECTS

An important goal of student projects in CS 401 was applying the principles of cybersecurity in a semester project. The projects also served two additional goals. First, the project allowed students to expand the core "T" of the course to satisfy their own passions and interests. For McDermott and O'Connell, this meant understanding how machine learning can be applied to improve cybersecurity. For Chen,
meant exploring how the security features of blockchain technology can be leveraged to transform business processes. Second, having students conduct independent research reinforces some of the essential cybersecurity concepts listed in Appendix A within a specific area. Thus, while the core “T” for every student in CS 401 was as summarized in Figure 4, the semester projects added depth in a way that customized the learning outcomes for each student as shown in Figure 5.

Using a distributed ledger, the privacy and security of transactions cannot be tampered with or篡改ed. This makes blockchain technology particularly suitable for applications that require high levels of both privacy and security. In the context of traditional financial institutions, blockchain technology can be used to improve the transparency and efficiency of the financial market, while also reducing fraud and errors. In the context of the retail industry, blockchain technology can be used to improve the traceability and transparency of supply chain, while also reducing the risk of product adulteration and counterfeiting. In the context of the healthcare industry, blockchain technology can be used to improve the privacy and security of patient data, while also reducing the risk of data breaches and unauthorized access.

**Figure 5.** CS 401 cybersecurity course “T” modified by select Essential Concepts from Appendix A

The title and a brief summary of each student project are presented below, followed by the six most prominent Essential Concepts (ECs, Burley & Bishop, 2017) covered by each project.

The ECs reinforced by the student projects were quite different. Two ECs are common to the McDermott and Chen projects – data integrity and authentication, and personal data privacy and security – and one EC – system monitoring – was common to the McDermott and OConnell projects.

**McDermott. Malware Identification and Protection on Mobile Devices Using Machine Learning**

This study reviews the current landscape of anti-malware security on Android mobile devices in the United States. There have been major breaches in confidentiality in recent years on smartphones, and there is now an increased need for safety due to users’ reliance on these devices. Based on current security standards, the requirements and expectations of users were discussed with regard to how they affect what security must be on a system. Google’s existing machine learning protocols in security were also reviewed. This study proposes the use of new machine learning methodologies to solve the four main issues (1) identification of mobile device vulnerabilities, (2) patching of vulnerabilities, (3) identification of malware on a device, (4) ways to remove malware from devices. The concepts of red-teaming, alerts, reinforcement machine learning, and virtual memory access patterns were covered as suggested ways to solve these issues. The implementation of these is described and an analysis of the “Gooligan” malware problem is reviewed with respect to these concepts.

**Most Significant ECs for McDermott:** Data integrity and authentication; Security requirements and their role in design; Static and dynamic testing; Configuring and patching; Personal data privacy and security; System monitoring

**OConnell. The Effectiveness of Behavior-Based Access Control: Mitigating Internal Threats at U.S. Financial Institutions**

Internal cyber threats at U.S. financial institutions present a significant concern due to the advantage held by insiders and the value of financial data and infrastructure. Currently, authorization management handled through traditional access control methods is insufficient for the dynamic networks and organizational systems of the twenty-first century. In response, behavior-based access control has been proposed as a solution, offering a dynamic and automatic access control system. To broaden our understanding of internal threats and the related benefits of behavior-based access control, this research aimed to 1) summarize the importance of considering internal threats, 2) identify the state of the art in behavior-based access control and its role in internal threat mitigation, 3) define challenges associated with the state of the art, and 4) present strategic practices and considerations for implementing these systems with consideration for financial organizations. This research aims to inform the evaluation of behavior-based access control and to provide background and considerations for decision makers determining whether to implement a system of this type.

**Most Significant ECs for OConnell:** Access control; Social behavioral privacy and security; Social engineering; Software component interfaces; System monitoring; Risk management

**Chen. Adoption of Blockchain Technology: The Healthcare Industry vs. Retail Industry**

Because of its potential to disrupt financial services and other industries, blockchain technology has the ability to be the ‘next internet’. The inherent benefits of built-in security...
coupled with the flexibility in different implementations allows for many applications and use cases. The acceptance of blockchain technology depends largely on the industry, its regulations, the use cases, and their relevant benefits. Blockchain technology was analyzed with respect to its benefits, risks, strengths and weaknesses in the context of two specific industries. The two industries explored are the healthcare industry, with a focus on healthcare data for the FDA and CDC, and the retail industry, with a focus on supply chain management for Walmart and Amazon. These two industries are used to assess the potential benefits and risks of blockchain by examining the opportunities and challenges in applicable use cases. This study concludes by formulating an outlook for blockchain adoption by these industries.

Most Significant ECs for Chen: Basic cryptography concepts; Data integrity and authentication; Personal data privacy and security; Governance and policy; Laws, ethics, and compliance; Supply chain management security

As can now be seen, the students participating in this course had varying focuses in their topics. Using the "T" shaped knowledge and skills provided by the course design, the students were able to develop and integrate these in very different ways. In a larger course setting this may lead to students having very similar knowledge areas enumerated within their "T"s, but there would likely be varying depths at which these topics are learned. In this example course, the students that had overlapping KAs almost certainly would give differing explanations of how these were integrated into their course projects.

We now explore issues beyond courses and projects. From an institutional perspective, we analyze and assess the current state of cybersecurity accreditation in the next section. From an educational perspective, we consider post-secondary certifications that are potentially helpful to students that pursue a career in cybersecurity in Appendix D.

5. ACCREDITATION

Cybersecurity accreditation is a work-in-progress (ABET, 2017; Yang & Wen, 2017; Wescott & Clark, 2017). ABET’s efforts to date have focused on six of the eight Knowledge Areas shown in Table 1, i.e. all except Component Security and Connection Security (ABET, 2017; Burley & Bishop, 2017; Wescott & Clark, 2017). It is an open question if these last two KAs will be added to the scope of ABET’s cybersecurity accreditation. AACSB’s efforts to date have been based on IS 2010. Within IS 2010, six of the seven core courses list some aspect of security as an important topic area:

- Foundations of Information Systems;
- Data and Information Management;
- Enterprise Architecture;
- IT Infrastructure;
- Systems Analysis and Design; and
- IS Strategy, Management, and Acquisition.

Furthermore, IS 2010 lists “IT Security and Risk Management” as one of a handful of important IS electives.

As of this writing, the most useful accreditation tools we have in the United States are the Center of Academic Excellence (CAE) designations from the National Security Agency (NSA, 2018b). The most popular of these designations is for Cyber Defense (CD).

The horizontal bar in Figure 6 contains what the NSA and Department of Homeland Security (DHS) call foundational KUs whereas the vertical bar contains core non-technical KUs (NSA, 2018a). Yang and Wen (2017) focus on non-technical NSA CAE-CD knowledge and skills in their study, as depicted in Figure 6, because of the connection between these eight Knowledge Units (KUs) and AACSB accreditation.
Institutions more focused on technical than managerial or behavioral knowledge and skills can leverage the NSA CAE-CD KUs shown in Figure 7. The horizontal bar in Figure 7 also contains the NSA’s three foundational KUs whereas the vertical bar contains five core technical KUs (NSA, 2018a). One of the strengths of NSA CAE-CD KUs is how comprehensive they are (Yang & Wen, 2017). In addition to the three foundational and ten core KUs shown in Figure 6 and Figure 7, institutions are encouraged to extend their offerings to include other KUs organized around specific focus areas (NSA, 2018a). Appendix C lists the 57 “optional” KUs that the NSA provides as guidance.

Finally, Westcott and Clark (2017) highlight the importance of ensuring that cross-cutting concepts are thoughtfully integrated into cybersecurity curricula for both pedagogical and accreditation purposes. For decades, these have included confidentiality, integrity and availability; the so-called CIA triad. Burley and Bishop et al. (2017) suggest that there is a need to expand this list of concepts from three to at least six:

- Confidentiality;
- Integrity;
- Availability;
- Risk;
- Systems thinking; and
- Adversarial thinking.

6. IMPLICATIONS AND CONCLUDING REMARKS

With some exceptions, if a science and technology story appears on the cover of Time Magazine (Vella, 2018) and is within a computing discipline, we should reflect on if and how we teach the topic at hand. This 2018 Time Special Edition does a nice job of presenting cybersecurity in a way that is accessible to its target audience and features actionable checklists for things that one should do at home (and at work) to improve one’s cybersecurity. But what do administrators and faculty need to understand about cybersecurity? We offer our reflections here with the understanding that these represent a more academic perspective than those of Time Magazine.

Implications for Administrators

Cybersecurity is emerging as a distinct discipline, even though it is tightly connected to all five of the computing disciplines shown in the lower half of Figure 3 as well as others, e.g., security analytics (Talabis, McPherson, Miyamoto, & Martin, 2015). This suggests that colleges and universities need to consider updating and revising curricula and courses in ways that go far beyond the security knowledge areas that their faculty learned as students (Newhouse, Keith, Scribner, & Witte, 2017; NIST, 2018). Although beyond the scope of our study, it is also important to consider the multidisciplinary nature of cybersecurity as suggested by the
interdisciplinary content examples shown at the top of Figure 3. We expect that many institutions can offer compelling, interesting and valuable courses that integrate two or more disciplines, e.g., human factors and cybersecurity; or policy, law, ethics and security; etc.

Because cybersecurity is an emerging discipline, the state of accreditation for cybersecurity is in flux. We recommend that administrators track the state of cybersecurity accreditation hand-in-hand with tracking advances and changes to curricula as they develop. For now, this likely means tracking ABET’s and AACSB’s activity and their progress in this area. There are also good reasons to consider applying for a National Security Agency Center of Academic Excellence in Cyber Defense or Cyber Operations (NSA, 2018b). Obtaining and supporting these designations (i.e., NSA CAE-CD and NSA CAE-CO), however, clearly will require institutional resources.

**Implications for Faculty**

Faculty teaching in computing disciplines are on the front lines of addressing what Simson Garfinkel calls “The Cybersecurity Mess,” which accurately describes the current state of affairs (Garfinkel, 2016; Vella, 2018). We encourage faculty to carefully consider the knowledge and skills they might design into their own “T-shaped” cybersecurity course, tailored to the institution or organization offering the course. Important questions here are how a course design matches the needs of the students as well as the requirements of their prospective employers. For the same stakeholders, it is also important to strike the right balance of technical and non-technical course content. Like the parts of a Banyan Tree (see Figure 1), the technical and non-technical components of cybersecurity are woven together and interconnected, as they are in information security (Cram & D’Arcy, 2016).

Faculty that are outside computer science departments can still add tremendous value by teaching their students cybersecurity using a T-shaped model. Applying this approach to course design and pedagogy will allow students to be more aware of the connections between domains, and also how they fit into knowledge areas. Integrating non-technical and interdisciplinary skills in courses outside of CS provides the opportunity to create more well-rounded students that understand how different essential concepts and topics can come together.

**Concluding Remarks**

More than 3 billion people are online (including bad actors) and more than 30 billion Internet of Things devices soon will be directly or indirectly connected to the internet. Furthermore, the digital transformation of modern enterprises makes information and communication technology (ICT) infrastructure mission critical. This ICT infrastructure therefore needs securing using a robust, holistic, and multidisciplinary approach, hence the horizontal stroke in our “T”.

But what about the vertical stroke in our “T”? From a science and technology perspective, cryptography and network security, as conceived in CS 401, are central to this urgent need.

In hindsight, we were pleased with the main text used in CS 401 (Stallings, 2017). As the title suggests, the strongest aspects of the Stallings (2017) book are its treatment of cryptography and network security. It is also adequate for teaching the basics within six of the eight cybersecurity Knowledge Areas shown in Table 1. It falls short, however, in providing adequate material for teaching organizational security and societal security. Another book that is just as technical as Stallings (2017) but provides broader coverage is Bishop (2018). Different books might be better for less technical Computer Information Systems majors than McDermott, O’Connell and Chen. For example, the texts (Pfleeger & Pfleeger, 2011) and (Whitman, Mattord, & Green, 2013) are explicitly mentioned as good examples in CS 2013 (Sahami & Roach, 2013). A different book would almost certainly be better for a more applied IS or IT major (Misra & Khurana, 2017). Three such examples are (Andress, 2014), (Boyle & Panko, 2014) and (Vacca, 2017). For minors in a computing discipline, Meeuwisse (2017) is an up-to-date and interesting alternative.

The supplemental readings for CS 401 in part balanced out the “T” shown in Figure 4. Only two of the five readings, however, were foundational in that they covered security operations at a high-level (NIST, 2018) and secure, tamper-resistant transactions, for example (Nakamoto, 2008). The remaining supplemental readings covered timely or more advanced topics (Bonneau & Miller, 2015; Chen, Paxson, & Katz, 2010; US DHS, 2016). If we were to teach this cybersecurity course again, supplemental readings that covered organizational security and societal security in general, and privacy in particular (Solove, 2010), would be welcome additions.

The authors are instructors or students at business schools in which management and governance of organizations is covered elsewhere in our respective curricula. However, special treatment of cybersecurity is inadequate or outdated in the courses at Bentley University and
West Texas A&M University, as we imagine it is in similar courses at other business schools that cover management, governance, or risk. Thus, teaching cybersecurity appears to be a critical area in which we can better serve our students. This paper is our attempt at raising awareness of the importance of teaching cybersecurity within a computing discipline and presents our approach to doing so mindfully. It remains an open question where cybersecurity fits in the landscape of higher education beyond computing disciplines. Furthermore, as younger generations are growing up as digital natives, we should also be asking what aspects of cybersecurity need to be taught in high school, middle school, or elementary school.

7. REFERENCES


# Appendix A – Joint Task Force on Cybersecurity Education

**Knowledge Areas [From CSEC 2017 Report aka (Burley & Bishop, 2017)]**

<table>
<thead>
<tr>
<th>Knowledge Area</th>
<th>Knowledge Units</th>
<th>Essential Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Security</strong></td>
<td>Cryptography</td>
<td>Basic cryptography concepts</td>
</tr>
<tr>
<td></td>
<td>Digital Forensics</td>
<td>Digital forensics</td>
</tr>
<tr>
<td></td>
<td>Data Integrity and Authentication</td>
<td>End-to-end secure communications</td>
</tr>
<tr>
<td></td>
<td>Access Control</td>
<td>Data integrity and authentication</td>
</tr>
<tr>
<td></td>
<td>Secure Communication Protocols</td>
<td>Information storage security</td>
</tr>
<tr>
<td></td>
<td>Cryptanalysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Privacy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information Storage Security</td>
<td></td>
</tr>
<tr>
<td><strong>Software Security</strong></td>
<td>Fundamental Principles</td>
<td>Fundamental design principles including least privilege, open design, and abstraction</td>
</tr>
<tr>
<td></td>
<td>Design</td>
<td>Security requirements and their role in design</td>
</tr>
<tr>
<td></td>
<td>Implementation</td>
<td>Implementation issues</td>
</tr>
<tr>
<td></td>
<td>Analysis and Testing</td>
<td>Static and dynamic testing</td>
</tr>
<tr>
<td></td>
<td>Deployment and Maintenance</td>
<td>Configuring and patching</td>
</tr>
<tr>
<td></td>
<td>Documentation</td>
<td>Ethics, especially in development, testing and vulnerability disclosure</td>
</tr>
<tr>
<td></td>
<td>Ethics</td>
<td></td>
</tr>
<tr>
<td><strong>Component Security</strong></td>
<td>Component Design</td>
<td>Vulnerabilities of system components</td>
</tr>
<tr>
<td></td>
<td>Component Procurement</td>
<td>Component lifecycle</td>
</tr>
<tr>
<td></td>
<td>Component Testing</td>
<td>Secure component design principles</td>
</tr>
<tr>
<td></td>
<td>Component Reverse Engineering</td>
<td>Supply chain management security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reverse engineering</td>
</tr>
<tr>
<td><strong>Connection Security</strong></td>
<td>Physical Media</td>
<td>Systems, architecture, models, and standards</td>
</tr>
<tr>
<td></td>
<td>Physical Interfaces and Connectors</td>
<td>Physical component interfaces</td>
</tr>
<tr>
<td></td>
<td>Hardware Architecture</td>
<td>Software component interfaces</td>
</tr>
<tr>
<td></td>
<td>Distributed Systems Architecture</td>
<td>Connection attacks</td>
</tr>
<tr>
<td></td>
<td>Network Architecture</td>
<td>Transmission attacks</td>
</tr>
<tr>
<td></td>
<td>Network Implementations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Defense</td>
<td></td>
</tr>
<tr>
<td><strong>System Security</strong></td>
<td>System Thinking</td>
<td>Holistic approach</td>
</tr>
</tbody>
</table>

---

©2019 ISCAP (Information Systems and Computing Academic Professionals)
https://isedj.org/; http://iscap.info
| System Management | Security policy
| Authentication | Access control |
| Access control | Monitoring |
| Recovery | Testing |
| System Testing | Documentation |
| Common System Architectures | |
| Human Security | Identity management |
| Social Engineering | Social engineering |
| Personal Compliance with Cybersecurity Rules / Policy / Ethical Norms | Awareness and understanding |
| Awareness and Understanding | Social behavioral privacy and security |
| Social and Behavioral Privacy | Personal data privacy and security |
| Personal Data Privacy and Security | |
| Usable Security and Privacy | |
| Organizational Security | Risk management |
| Security Governance and Policy | Governance and policy |
| Analytical Tools | Laws, ethics, and compliance |
| Systems Administration | Strategy and planning |
| Cybersecurity Planning | |
| Business Continuity, Disaster Recovery, and Incident Management | |
| Security Program Management | |
| Personnel Security | |
| Security Operations | |
| Societal Security | Cybercrime |
| Cyber Law | Cybercrime |
| Cyber Ethics | Cyber law |
| Cyber Policy | Cyber ethics |
| Privacy | Cyber policy |
| | Privacy |
Appendix B – Cybersecurity Course Syllabus

Bentley University – Computer Information Systems Department
CS 401 – Cybersecurity
Spring 2018 Syllabus

Instructor: David J. Yates
E-Mail: dyates@bentley.edu
Class Meeting: Monday & Thursday 11:00 AM – 12:20 PM
Location: Our classroom
Office Hours: By appointment

Course Overview

Prerequisites
A networking, operating systems or computer architecture course.

Required Materials

In addition to the required textbook, supplemental readings and other material will be provided on Blackboard.

Course Description
This course provides a technical focus on information, computer, and network security, which together form the basis for cybersecurity. It introduces what cybersecurity means, both in the abstract and in the context of real-world information systems. Students learn relevant cybersecurity principles, practices, technologies, and approaches. Students recognize and understand threats to confidentiality, integrity and availability as well as best-practices to defend against such threats.

Course Objectives
Upon successful completion of the course and the assignments, it is expected that the student will:

1. Develop a basic understanding of cybersecurity, how it has evolved, and best practices for cybersecurity used in modern enterprises.
2. Develop an understanding of cybersecurity as practiced in hardware, operating systems, virtual machines, distributed information systems, networks, and representative applications.
3. Gain familiarity with prevalent network and system attacks, defenses against them, and forensics to investigate the aftermath.
4. Develop an understanding of security policies as well as mechanisms to implement and assure such policies.

**Teaching Methods**

1. **Lectures and Discussion:** Important material from the class notes and outside sources will be covered in class. Students should plan to take careful notes as not all material can be found in the handout class notes or class examples. Discussion is strongly encouraged as is reading online material relevant to topics being covered. Students are required to read all the materials assigned as scheduled.

2. **Project and Project Milestones:** Four project-based assignments are given across the semester, each reflecting the development of the project in phases. These project milestones should be submitted via the course Blackboard site. You should feel free to consult with me and others for help, and even consult with your contacts in this area. However, please be sure to submit your own work and cite all external sources properly. For example, students are expected to develop a project proposal, which will be submitted on February 25. Finally, submitted work will be checked by turnitin.com.

3. **Exams:** Two in-semester exams plus a final exam will be given, covering the material in the readings, discussions and textbook. You are responsible for answers and insights drawn from material that will be covered in the discussions, but may not be in the book.

4. **Internet/Blackboard Site:** All material including class notes, instructional material, and student assignments will be distributed on the Bentley University Blackboard web site. Grades for assignments and exams will also be posted on the Blackboard web site.

**Course Policies**

**Evaluation**

The final course numerical grade will be based on the following components (shown with weights):

<table>
<thead>
<tr>
<th>Component</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-semester Exams</td>
<td>25%</td>
</tr>
<tr>
<td>Project Proposal and Presentation</td>
<td>15%</td>
</tr>
<tr>
<td>Class Participation</td>
<td>10%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>20%</td>
</tr>
<tr>
<td>Final Project, Due May 8</td>
<td>30%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

The Bentley University Grading System will be used to determine the final letter grade.
Students are to keep track of class standing throughout the semester. It is important to discuss any significant issues with the Instructor before the end of the course.

**Coursework**

Students must read the assigned material before class and be prepared to participate in class discussions. Meaningful class participation and general interest in the course will also influence the final course grade. Students are expected to ask and answer questions as well as to offer worthwhile observations on the subject matter under discussion. In addition to participating actively and constructively in class, students must cooperate with team members in any group activities assigned during the term.

**Attendance**

Students are expected to attend every class. Missed classes will lower your final grade.

**Academic Integrity**

**Bentley University Honor Code**

The Bentley University Honor Code formally recognizes the responsibility of students to act in an ethical manner. It expects all students to maintain academic honesty in their own work, recognizing that most students will maintain academic honesty because of their own high standards. The honor code expects students to promote ethical behavior throughout the Bentley University community and to take responsible action when there is a reason to suspect dishonesty.

In addition, the honor code encourages faculty members to foster an atmosphere of mutual trust and respect in and out of the classroom. Faculty are also expected to share the responsibility of maintaining an academically honest environment.

The honor code is not meant to be a cure for all occurrences of academic dishonesty. It does not seek to create a community of informers. Rather, the honor code depends upon the good will to care enough for a friend or a fellow student, even a stranger, to warn the individual to abandon dishonesty for the individual’s own sake and that of the community. Thus, the honor code asks all students to share the responsibility of maintaining an honest environment.

The students of Bentley University, in a spirit of mutual trust and fellowship, aware of the values of a true education and the challenge posed by the world, do hereby pledge to accept the responsibility for honorable conduct in all academic activities, to assist one another in maintaining and promoting personal integrity, to abide by the principles set forth in the honor code, and to follow the procedures and observe the policies set forth in the academic integrity system.

**The Bentley University Honor Code and this Class**

With regard to citation:

- Work done by others should be properly cited. Committing plagiarism is forbidden by the Bentley University Honor code: copying information, ideas, or phrasing of another person without proper acknowledgment of the true source; writing or presenting as if it is your own information, ideas, or phrasing without proper acknowledgment of the true source are all forbidden.

- Using a commercially-prepared paper or research project or submitting for academic credit any work completed by someone else is also forbidden.
With regard to collaboration:

- Homework assignments and the final project are individual efforts. Students may discuss ideas, but the assignments and writing must be done individually.
- Using work done by another student in an earlier semester is not allowed.

You are responsible for seeking clarification from the Instructor for any of the criteria you do not understand.

**Learning Disabilities**

I adopt the Bentley University commitment to social justice and expect to foster a nurturing learning environment based upon open communication, mutual respect, and non-discrimination. Our University does not discriminate on the basis of race, sex, age, disability, veteran status, religion, sexual orientation, color or national origin. Any suggestions as to how to further such a positive and open environment in this class will be appreciated and given serious consideration. If you are a person with a disability and anticipate needing any type of accommodation in order to participate in this class, please advise me as soon as possible, and make appropriate arrangements with the Office of Disability Services in Jennison (also at 781-891-2004).

**Course Schedule**

<table>
<thead>
<tr>
<th>Week / Day</th>
<th>Topic</th>
<th>Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1 (Jan 18)</td>
<td>Course structure. Introduction to cybersecurity concepts: Security architecture, models, standards (ISO, NIST), attacks, services, policies, mechanisms. Design principles, attack surfaces, trees.</td>
<td>Chapter 1</td>
</tr>
<tr>
<td>Week 2 (Jan 22 &amp; 25)</td>
<td>Encryption techniques: Symmetric ciphers, substitution, transposition, rotor machines, steganography.</td>
<td>Chapter 3</td>
</tr>
<tr>
<td>Week 3 (Jan 29 &amp; Feb 1)</td>
<td>Block ciphers and DES: Block cipher structure, DES encryption and decryption, strength of DES. Block cipher design.</td>
<td>Chapter 4</td>
</tr>
<tr>
<td>Week 4 (Feb 5 &amp; 8)</td>
<td>Advanced Encryption Standard (AES): Finite fields, AES structure, transformation functions, key expansion. AES implementation.</td>
<td>Chapter 6</td>
</tr>
<tr>
<td>Week 5 (Feb 12 &amp; 15)</td>
<td>Block cipher operation: Multiple encryption and Triple DES, electronic codebook, cipher block chaining, cipher feedback mode, output feedback mode, counter mode (ECB, CBC, CFB, OFB, CTR). XTS-AES for block storage, format-preserving encryption.</td>
<td>Chapter 7</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Week 6 (Feb 19 &amp; 22)</td>
<td>Random bit generation and Stream Ciphers: Pseudorandom numbers, generation using a block cipher. Stream ciphers, RC4, truly random numbers.</td>
<td>Exam 1</td>
</tr>
<tr>
<td>Week 7 (Feb 26 &amp; Mar 1)</td>
<td>Public key cryptography and RSA: Public key cryptosystems, principles and practices, RSA algorithm.</td>
<td>Chapter 8</td>
</tr>
<tr>
<td>Week 8 (Mar 12 &amp; 15)</td>
<td>Cryptographic hash functions: Applications, examples, requirements and security, hash functions using CBC. Secure hash algorithms, SHA-3.</td>
<td>Chapter 11</td>
</tr>
<tr>
<td>Week 9 (Mar 19 &amp; 22)</td>
<td>Digital signatures: Elgamal and Schnorr schemes. NIST, RSA-PSS and Elliptic Curve algorithms.</td>
<td>Chapter 13</td>
</tr>
<tr>
<td>Week 10 (Mar 26 &amp; 29)</td>
<td>Key management and distribution: Symmetric key distribution two ways (using symmetric and asymmetric encryption). Distribution of public keys, X.509 certificates, PKI.</td>
<td>Chapter 14</td>
</tr>
</tbody>
</table>
| Week 13  
(Apr 17 & 19) | What’s new about cloud computing security? Definition confusion, history, what is not new, what is new, cloud threats, opportunities. Strategic principles for security the Internet of Things (IoT): Overview, principles, practices, guidance. | Supplemental Readings II, III |
| Week 14  
| Week 15  
(Apr 30) | **Final Project Presentations** | |
| (May 3) | **Final Exam** | |
| (May 8) | **Final Project Reports** | Submit project final report to blackboard (TurnItIn.com) by 11:59 PM |
# Appendix C – U.S. National Security Agency Cyber Defense Knowledge Units for Centers of Academic Excellence (NSA, 2018a)

## Centers of Academic Excellence in Cyber Defense (CAE-CD)

<table>
<thead>
<tr>
<th>Foundational KU’s</th>
<th>Technical Core KUs</th>
<th>Non-technical Core KUs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Foundations</td>
<td>Cybersecurity Foundations CSF</td>
<td>Cyber Threats</td>
</tr>
<tr>
<td>Cybersecurity Principles</td>
<td>Cybersecurity Principles CSP</td>
<td>Cybersecurity Planning and Management</td>
</tr>
<tr>
<td>IT Systems Components</td>
<td>IT Systems Components ISC</td>
<td>CPM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Optional KU’s</th>
<th>Optional KU’s</th>
<th>Optional KU’s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Algorithms</td>
<td>Advanced Algorithms AAL</td>
<td>Intrusion Detection/Prevention Systems</td>
</tr>
<tr>
<td>Advanced Cryptography</td>
<td>Advanced Cryptography ACR</td>
<td>IDS</td>
</tr>
<tr>
<td>Algorithms</td>
<td>Analog Telecommunications ATC</td>
<td>Linux System Administration LSA</td>
</tr>
<tr>
<td>Cloud Computing</td>
<td>Basic Cyber Operations BCO</td>
<td>Mobile Technologies MOT</td>
</tr>
<tr>
<td>Cyber Crime</td>
<td>Cloud Computing CCO</td>
<td>Network Forensics NWF</td>
</tr>
<tr>
<td>Cybersecurity Ethics</td>
<td>Cyber Crime CCR</td>
<td>Network Security Administration NSA</td>
</tr>
<tr>
<td>Data Administration</td>
<td>Cybersecurity Ethics CSE</td>
<td>Network Technology and Protocols NTP</td>
</tr>
<tr>
<td>Digital Forensics</td>
<td>Data Administration DBA</td>
<td>Operating Systems Hardening OSH</td>
</tr>
<tr>
<td>Embedded Systems</td>
<td>Data Structures DST</td>
<td>Operating Systems Theory OST</td>
</tr>
<tr>
<td>Database Management Systems</td>
<td>Database Management Systems DMS</td>
<td>Penetration Testing PTT</td>
</tr>
<tr>
<td>Databases</td>
<td>Databases DAT</td>
<td>Privacy PDI</td>
</tr>
<tr>
<td>Device Forensics</td>
<td>Digital Communications DCO</td>
<td>QA/Functional Testing QAT</td>
</tr>
<tr>
<td>Digital Forensics</td>
<td>Digital Forensics DFS</td>
<td>Radio Frequency Principles RFP</td>
</tr>
<tr>
<td>Embedded Systems</td>
<td>Digital Forensics DFS</td>
<td>Secure Programming Practices SPP</td>
</tr>
<tr>
<td>Forensic Accounting</td>
<td>Embedded Systems EBS</td>
<td>Software Assurance SAS</td>
</tr>
<tr>
<td>Formal Methods</td>
<td>Forensic Accounting FAC</td>
<td>Software Reverse Engineering SRE</td>
</tr>
<tr>
<td>Fraud Prevention and Management</td>
<td>Formal Methods FMD</td>
<td>Software Security Analysis SSA</td>
</tr>
<tr>
<td>Hardware Reverse Engineering</td>
<td>Fraud Prevention and Management FPM</td>
<td>Supply Chain Security SCS</td>
</tr>
<tr>
<td>Hardware/Firmware Security</td>
<td>Hardware Reverse Engineering HRE</td>
<td>Systems Certification and Accreditation SCA</td>
</tr>
<tr>
<td></td>
<td>Hardware/Firmware Security HFS</td>
<td>Systems Programming SPG</td>
</tr>
<tr>
<td>Course Title</td>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Host Forensics</td>
<td>HOF</td>
<td>Systems Security Engineering</td>
</tr>
<tr>
<td>IA Architectures</td>
<td>IAA</td>
<td>Virtualization Technologies</td>
</tr>
<tr>
<td>IA Compliance</td>
<td>IAC</td>
<td>Vulnerability Analysis</td>
</tr>
<tr>
<td>IA Standards</td>
<td>IAS</td>
<td>Web Application Security</td>
</tr>
<tr>
<td>Independent/Directed Study/Research</td>
<td>IDR</td>
<td>Windows System Administration</td>
</tr>
<tr>
<td>Industrial Control Systems</td>
<td>ICS</td>
<td>Wireless Sensor Networks</td>
</tr>
<tr>
<td>Introduction to Theory of Computation</td>
<td>ITC</td>
<td></td>
</tr>
</tbody>
</table>
Appendix D – Cybersecurity Certifications

Comprehensive cybersecurity certifications are currently in development. The organization with the longest track record of offering certifications to security professionals is the International Information System Security Certification Consortium, or (ISC)². (ISC)²’s most popular certification is the Certified Information Systems Security Professional (CISSP), which, as the name implies, is rooted in information security more so than cybersecurity (Grover, Reinicke, & Cummings, 2015). However, revisions to the CISSP common body of knowledge (CBK) in 2015 and 2018, combined with a work experience requirement, have maintained the relevance and rigor of this certification (Chappell, Stewart, & Gibson, 2018). According to (ISC)²’s website (https://www.isc2.org) a CISSP candidate today “must have a minimum of five years cumulative paid work experience in two or more of the eight domains of the CISSP CBK. Earning a four-year college degree or regional equivalent or an additional credential from the (ISC)² approved list will satisfy one year of the required experience. Education credit will only satisfy one year of experience.” Figure 8 depicts the eight domains in the CISSP CBK as the horizontal stroke of the “T” because of the breadth of knowledge required to obtain this certification.

![Figure 8: Example of stacked (ISC)² certifications for cybersecurity professionals. The horizontal stroke of the “T” represents the CISSP. The vertical stroke represents the CCSP.](image)

Although (ISC)² does not have a certification that carries the cybersecurity name, the CISSP can be supplemented with other certifications, from (ISC)² or other organizations, e.g., ISACA or CompTIA (Grover, Reinicke, & Cummings, 2015; Hartley, Medlin, & Houli, 2017; NIST, 2018), to more closely match what a cybersecurity professional might need to know. The vertical stroke of the “T” in Figure 8 shows one such illustrative example by including the six domains covered in the (ISC)² Cloud Computing Security Professional (O’Hara & Malisow, 2017) common body of knowledge (CCSP CBK). Obtaining the CCSP requires at least three years of work experience in information security and one year in one or more of the six domains shown on the vertical in Figure 8.

The choice of the CCSP in Figure 8 is one of several practical (and marketable) alternatives to demonstrate and certify depth in a specific area (Burley & Bishop, 2017; Wescott & Clark, 2017). As another example, the Information Systems Security Engineering Professional (ISSEP), which is one of three CISSP follow-on certifications, and dubbed the CISSP-ISSEP (Chappell, Stewart, & Gibson, 2018; Ross, McEvilley, & Oren, 2018), is popular among professionals working in the U.S. defense industry. This certification requires at least two years of work experience in one or more of the five domains within the ISSEP common body of knowledge.
In sum, for students that wish to continue their education and training after college, the CISSP and related certifications provide high-quality, cross-industry, and vendor-agnostic certifications that typically will serve them well (Grover, Reinicke, & Cummings, 2015; Hartley, Medlin, & Houlik, 2017; Newhouse, Keith, Scribner, & Witte, 2017; Wescott & Clark, 2017).