Cybersecurity for MBAs: Pi-shaped Course Design

William W. Agresti
agresti@jhu.edu

Carey Business School
Johns Hopkins University
100 International Drive
Baltimore, MD 21202

Abstract - This article addresses the need for cybersecurity-savvy business leaders by describing the design of a cybersecurity course for students pursuing the MBA and other business degrees. Design drivers and the context for delivery led to a unique pi-shaped course design. The top horizontal bar of the pi symbol represents cybersecurity scope: students gaining an understanding of the breadth of the subject with guiding frameworks and models. The two vertical legs in the pi symbol provide opportunities for students to achieve depth: (1) cyber assess, for student teams to assess the cybersecurity state of a real organization, and (2) cyber brief, for teams to conduct research and analysis on specific cybersecurity topics of interest. Experiences with offering the course are discussed, with lessons learned and recommendations for continued improvement.

Categories and Subject Descriptors

K.3.2.b Computer Science Education; K.4.4.f Security; K.6.1.b Management Techniques

General Terms

Education, Security

Keywords

Education, Security, Security Management, MBA

1. INTRODUCTION

In the run of recent data breaches, Target's 2013 breach stands out because the CEO got fired. If the corporate world ever needed a wake-up call that cybersecurity is more than a technical issue, this was it. Those of us working in this field have long recognized the key roles for policy, processes, and leadership in cybersecurity, but this reality is now more widely understood than ever before.

With the important capacity-building initiatives in cybersecurity [1], it is natural to focus on the acute need for technical professionals. However, cybersecurity management and security-savvy business leaders are also sorely needed. This concurrent concern on cybersecurity's non-technical front has prompted education and training providers to offer courses and entire degree programs that emphasize cybersecurity management [2].

Educational attempts to bridge cybersecurity and management must consider continuing cybersecurity changes and the management approaches to deal with them. For one academic option, information security MBA programs [3], it would seem especially challenging to design - and keep current - an entire curriculum of courses. This article reports on experiences with another kind of entry in this cybersecurity management space: a single cybersecurity course in an MBA program.

While this course is aimed at current and future business leaders, it also addresses cybersecurity education and workforce initiatives. The National Cybersecurity Workforce Framework [1] is organized into seven high-level categories; 31 specialty areas; competencies; knowledge, skills, and abilities (KSAs); and tasks. To place this course in context, it addresses needs in the category titled "Oversight and Development" and specialty areas of "Security Program Management" and "Strategic Planning and Policy Development." The learning objectives of this course support attainment of five of the framework competencies: External Awareness; Legal, Government, and Jurisprudence; Organizational Awareness; Risk Management; and Technology Awareness.

We describe the design drivers for the course, its learning objectives and delivery strategies, the resulting pi-shaped course design, lessons learned, and

recommendations, with the intention that these observations may be useful in our efforts as a community to develop effective courses and programs for cybersecurity leadership and management.

2. DESIGN DRIVERS FOR THE COURSE

Several factors figured prominently in the design of the course. The context was that courses in the school are 2-credits, with 24 contact hours in a traditional classroom setting (or online) over eight weeks. This quarter system format is not unusual in business schools. The course is currently offered in-class, serving students pursuing an MBA and various business-related MS programs in both full-time and part-time formats. Given the demands from their major fields of study, most students only take this single course in cyber. So, for a single course in this restricted timeframe, an admittedly self-serving emotion was that this course design challenge was particularly difficult by analogy with it being tougher to give a five-minute talk than a one-hour one. There are so many possibilities for what to do in the eight class sessions, that this cybersecurity course would be a test of "professor as curator," seeking to identify and integrate just the right elements to make a unifying and effective treatment of the subject and, more to the point, a worthwhile learning experience for students.

Offered within a business school, this cybersecurity course is decidedly different from microeconomics or corporate finance. Our subject is more routinely in flux, and in the daily news: "backdoors" for encrypted smartphones, ransomware, cyberattacks on companies, cyberterrorism, cybercrime, invasions of privacy, security-related legislation, identity theft, stolen intellectual property, and the evolution and control of the Internet. So it is especially critical for a course like this to use the best course-design practices, such as,

- Backward Design: What are the learning objectives and outcomes for the course? With so many possibilities for topics, what do we want students to know and know how to do when they leave the course? And five years later? Given these objectives and outcomes, what set of learning activities, and organization of those activities in the course, will work best?

- Leveraging External Resources and Learning Technologies: How can we best make use of existing documents, research findings, technology demonstrations, simulations, interactive learning modules, videos, webinars, online meetings, etc., including externalizing our own resources, such as by recording short lecture modules and flipping the classroom? What learning models will work best to enable students to attain the learning objectives? What assessments will give us confidence about the nature and extent of student learning?

A particular concern was that, because of the breadth of the subject, it seemed entirely possible for the class to "rummage around" on the surface of cyber - e.g., discussing the many current events - such that, when the course was completed, the students would be no closer to having confidence in their understanding of cybersecurity than if they had never taken the course.

An additional design factor was that we wanted as many students as possible to take this elective course so more future business leaders would have a basic understanding of cybersecurity. So we have no prerequisite for the course. We want the course to be accessible - and students to be able to succeed in the course - without specific prior knowledge beyond being admitted to a graduate business program. We anticipated, and this was borne out, that many prospective students were apprehensive about choosing cybersecurity as an elective because they perceived this as a technical subject, with attendant expectations that all students must be good programmers and very strong in mathematics and technical subjects.

With cybersecurity, we were intent on wanting learning outcomes beyond one year of students completing the course. This meant identifying frameworks and models that have persistence over time, so students can place new technologies and policies into an evolutionary context – and know places to look for ongoing knowledge and guidance. So an overarching learning objective was that students leave the course with a deeper understanding, than someone who did not take the course, of the essential issues that underlie current news and events related to security and privacy. Is end-to-end encryption a slam dunk for organizations? We

want our students to know how some companies discovered critical IP leaving their networks undetected because the data was encrypted.

Here is the way we addressed the questions above. For our resulting course learning objectives, we wanted students, by the end of this course, to be able to:

- Describe the various ways that cybersecurity influences the success of global organizations
- Demonstrate a fundamental understanding of cybersecurity models, concepts, issues, and principal components
- Incorporate multiple perspectives in planning cybersecurity controls to address vulnerabilities
- Plan a cybersecurity assessment program for an organization
- Participate effectively as a member of a team to develop cybersecurity priorities for an organization

To construct the teaching-learning environment so students can attain these objectives, we considered various learning models (e.g., the five models in [4]), resulting in a hybrid model with emphasis on the information-processing model family. Our learning activities featured required readings and short case studies before in-class brief lecture modules that are designed to raise questions for immediate discussion. We arrange for guest speakers, but use them judiciously, given the limited class meeting time. Our online discussion boards enable extended asynchronous discussions and a way to post links to news stories, research results, etc. The flexibility for students to raise points of interest extends to the classroom, where they bring in topics for discussion. We use multiple in-class exercises – some individual and some using small groups of students – that have worked well as a way to address privacy, policy, and ethical issues in security. We also have found some existing videos that demonstrate the operation of some cybersecurity technologies, so students can view them outside of class.

To assess learning, we constructed rubrics for all assignments and showed the students the rubrics ahead of time. In addition to the assessment of the team

deliverable products and oral presentations, we assess individual learning using written assignments and examinations with short essay questions or case analyses that address students' ability to integrate across their learning and develop ideas and approaches to address the circumstances raised in the questions. We haven't been offering the course long enough to get at the value of the course several years after students have taken it. In the meantime, we examine the results of broader-scale alumni surveys for comments about the course, and we check with graduates informally for their suggestions on improving the course, based on their experiences after graduating.

3. COURSE STRATEGIES TO ADDRESS CYBERSECURITY IN AN ORGANIZATION

Considering our orientation to educating business leaders, our context was cybersecurity for an organization. As our students serve as business professionals and leaders, we want their understanding of cybersecurity to inform their activities and decisions as they work to make organizations successful. This cybersecurity understanding includes having an awareness of how much more there is to the subject and where to go to find it, knowledge that may help with bringing in new employees and external expertise and resources. As a research university, we introduce research results throughout the course. This research orientation supports an ongoing thread in the course to understand the degree of confidence in the sources of information on which to base cybersecurity understanding and decision-making.

Our course learning activities implement the strategies of establishing an executive-level perspective of cybersecurity and understanding internal and external drivers for an organization's cybersecurity program.

- Take on a C-level cybersecurity perspective

  We want students to address the challenge of how to assess cybersecurity from the vantage point of an entire organization. This enterprise-level perspective immediately triggers a useful consideration for students about the size and complexity of various enterprises. For large global

corporations, what are the best organizational units to have cybersecurity programs and then have these programs collaborate? Can the structure of an enterprise cybersecurity program take advantage of the implementation of other enterprise-wide operations, such as governance, compliance, and enterprise risk management?

As a business leader, what are reasonable ways to say something meaningful about the state of cybersecurity in an organization? A recent news headline said that Canada's cybersecurity readiness was 77% [5]. What does that mean? We are saying that effective characterization of an organization's cybersecurity is a challenge, yet here we have a quantitative assessment for an entire country!

Does spending more money on cybersecurity yield measurable improvements? An affirmative answer means that we have some way to gauge improvement. Does a company's enhanced security lead to higher profits because customers choose that company's products and services over competitors? If an organization boasts that its security is better than its competitors, as some banks and financial institutions do, what are the consequences? Do those companies become more at risk because they are more attractive targets for hackers? What does the research say about the impact of data breaches? On revenue? On stock price? On market share? How long does it take for a company to recover from a breach?

- Identify internal and external cybersecurity drivers

  Looking internally is to encourage the development of a cybersecurity program that makes sense for a particular organization. What is its mission and vision? What assets does it need to protect? How secure does it want / need to be? Questions like this can be useful to spark discussion around the myth of being 100% secure and the question of what other percentages would even mean. What is it about an organization that drives its cybersecurity program? Does the company handle healthcare data? Does it have electronically linked supply chains with vendors and customers?

The external view examines laws, regulations, and standards that apply to an organization. What levels of diligence and compliance must be maintained for ongoing operations? What does an external environmental scan say about important developments that are meaningful to the company, such as news reports of cybercrime, data breaches, and new technologies? What is the latest on the positions of tech companies and governments regarding the use of encryption? What do industry analysis firms say about trends and cybersecurity service providers? What are key results from the cybersecurity research community? How can an organization benefit from information sharing, e.g., via cyber-related Information Sharing and Analysis Centers (ISACs) [6].

An external orientation includes discussing how cybersecurity leaders in organizations often establish and cultivate relationships with their counterparts at similar organizations. We are cautious about the overused "best practices" label, but what are the effective practices of peer organizations that expert outsiders would consider competent and responsible? These peer networks may operate at various levels of formality. They may include sharing in formal benchmarking arrangements, so individual firms can get some calibration for how they are doing compared to their peers. Or they may be informal "round tables" where they can share experiences in a trusted setting: what new products are working well or not? What trends are they seeing at their firms? Having such networks can facilitate providing students with general ideas of how company cybersecurity programs operate.

These contextual factors and overall course strategies drove us to a distinctive pi-shaped design for our cybersecurity course.

4. PI-SHAPED COURSE DESIGN

The "pi-shape" metaphor was perhaps more prominent in our minds with our business school context. The story begins with a criticism that higher education was turning out I-shaped graduates: possessing disciplinary strength but lacking in other

knowledge and skills that would help them be successful in business. What was needed were T-shaped graduates who still had strength in one discipline but also had, by the top bar of the T, some knowledge and understanding of other disciplines and perspectives. These T-shaped professionals could collaborate and innovate across disciplines for the betterment of their organizations. And now the progression should be becoming clearer that, in these complex global business environments, we need to add another leg to the T. Enter the pi-shaped professional. There are various options for what this second leg could be. It may be establishing the importance of so-called right-brained thinking, a competence with behavioral soft-skills, or experience in a domain such as energy, consumer packaged goods, or manufacturing. So, a pi-shaped business school graduate would have depth in one discipline (e.g., in marketing or finance), coupled with a working knowledge of parallel disciplines, sufficient background in a domain, an understanding of human and organizational behavior, and the skills and dispositions to work effectively in pursuit of the company mission. Wow!

We embraced the imagery of the pi-symbol to visualize the perceived need for both depth and breadth in the outcomes of the cybersecurity course in rough analogy to its use above. The top horizontal bar of the pi-symbol would attend to the necessary breadth that exists in this subject of cybersecurity. The strong feeling during the course design process was that stopping at this point would be a mistake, leaving students with a surface understanding, without the opportunity to "roll up their sleeves" and dig into any single aspect of cyber. Furthermore, even a single detailed probe (T-shape) would not be sufficient. So, one leg of the pi-symbol would be a student team assessing the cybersecurity profile of a real organization and deciding how to improve it. The second leg would be the same team investigating a specific cybersecurity topic in depth. These two vertical legs of the pi-symbol would also support the learning objectives of students working in a team setting, sharing their knowledge and experiences, and applying them to new challenges.

Students at our school have diverse backgrounds, so we are helped out in forming teams that reflect that diversity. To help further with diversity, we have

made assignments of students to teams rather than having students form teams on their own. By using teams of students with diverse backgrounds, the students will be modeling behavior that we discuss in class about the benefits of using diverse teams in organizations to assess cybersecurity. Many of the cybersecurity risk management and assessment frameworks [7] make a point about industry teams not being viewed solely as comprised of IT and security professionals. There are benefits from having employees representing all parts and hierarchical levels of an organization. In particular, as noted in [8], cybersecurity is everybody's business, not just the IT and security professionals. For example, an administrative support person may be uniquely able to provide the solution to a data integrity problem: modify the user interface so employees can review their database changes before submitting them.

4.1 Horizontal Bar in Pi: Cyber Scope -- Breadth, Frameworks, and Models

Addressing the top bar means guiding students to an understanding of the scope and breadth of cybersecurity, which means different things to different people and entities [9]. Given that October is Cybersecurity Awareness Month in the US, cybersecurity is obviously thought to have relevance for the general public, while also having special meaning for different communities, such as law enforcement and national defense. We wanted students, after completion of the course, to be able to discuss thoughtfully the many aspects that comprise cybersecurity. This is not memorizing a textbook definition, but rather helping their colleagues with a sense of what cybersecurity means – for countries, for organizations, for individuals. For example, one aspect of understanding cybersecurity is to examine its relationships to other items on the senior leadership agenda, such as governance, risk, compliance (GRC) and enterprise risk management (ERM).

After developing a working definition that encapsulates the breadth and diverse elements of cyber, we next examine frameworks and models that can offer some stability to a rapidly changing field by representing the various constituent elements of cybersecurity and their inter-relationships. The McCumber cube [10], cybersecurity Essential Body of Knowledge (EBK) [11], the NIST framework [12], and standards like ISO 27001 [13] are examples of useful models in this regard. After

the course is over, students may be able to recognize new cybersecurity developments as fitting into the models we discussed in class. While the frameworks offer some stability in overall structure, we also highlight their dynamic nature as framework elements and inter-relationships evolve to keep pace with changes in the field.

Frameworks also serve as ways to deconstruct cybersecurity for operational use. For example, while NIST describes hundreds of security controls, we focus on how they are grouped into 18 families of controls [14]. In contrast to a laundry list of threats, we introduce threat taxonomies, such as the one from SEI [15], with its four classes of threats: actions of people, systems and technology failures, failed internal processes, and external events. For cybersecurity risk assessments, there are several frameworks [7] that can provide structure. As a link to the later student team activity of assessing an organization's cybersecurity, these various decompositions (e.g., from [13] into business continuity planning, system access control, asset classification and control, et al.) can provide the basis for auditing an organization's effectiveness regarding each element, and rolling up the results into an overall assessment for the enterprise. These explorations have the useful side effect of adding new entries to our class's running list of the abundant terminology in our field.

In addition to introducing persistent frameworks, we recommend assigning classic readings. Ross Anderson and Tyler Moore's article in *Science* [16] was a milestone, signaling the legitimacy of the economics of security as an enormously challenging subject worthy of research attention. This recommendation is in the same spirit as Chuck Pfleeger pointing out recently [17] that Saltzer and Shroeder's eight core principles of security are still valid forty years after publication [18].

The defining cybersecurity infrastructure framework is the Internet itself, with its architecture and protocols. Of special relevance to cybersecurity is to discuss the origin of the Internet. Its intended purpose and using community quite understandably led to an architecture that did not give prominence to security concerns and, instead, used features that are exploited today for illegal and malicious intent. These observations lead naturally to a discussion of packet switching and TCP/IP and the challenges of attribution for malicious and criminal activity over

the Internet. Of particular relevance to cybersecurity in an organization is a discussion of access via the Internet to private data on company networks: surface web and deep web.

With the cyber scope horizontal bar showing the breadth, the two legs in the pi-symbol are deep dives into selected aspects of cybersecurity so that students get beyond the surface and have a chance to probe topics in detail.

4.2 First Leg in Pi: Cyber Assess – Controls, Assets, Threats, Vulnerabilities (CATV)

One leg provides for student teams to take on the challenge of structuring a cybersecurity program for a real organization. Setting up this learning activity meant identifying a public or private organization of appropriate size: not so large as to require the teams to spend excessive time to understand its mission and operations, yet not so small as to be a trivial exercise.

The structure for this leg of cybersecurity assessment is Controls, Assets, Threats, and Vulnerabilities (CATV). We discuss topics in this order, and student teams concurrently relate this class work to their assignment.

Beginning with controls, the first realization for teams is that this selected organization will already have controls in place. The team probe into the organization may be starting from scratch, but a useful learning opportunity is for teams to consider the set of controls that may be expected to be installed and operative. We benefit from the analogy that students have routine controls on their laptops, to include means of authentication such as passwords, ways to lock and unlock their laptop, and security software for malware. How do these same properties of authentication, access control, and malware detection carry over to an entire organization?

As teams settle on this first set of assumed controls, basic hygiene for the organization, it offers a link to the business issue of spending for security. Is such spending a routine expense of doing business or an investment? What kinds of spending beyond the basic controls can be considered an investment? To what

extent can cost-benefit analysis, capital budgeting models, and even real options, provide assistance in these decisions?

Continuing with the controls topic, we keep building from familiar terms like firewalls to consider the various categories of controls, helped out by frameworks like the one from SANS [19]. For this cyber assess activity, we consider controls liberally as any interventions that are directed at improving cybersecurity in the organization. So this includes training, biometrics, education, policies, encryption, procedures, business continuity, disaster recovery, strategic alliances, et al. Completing the treatment of controls should leave students with an appreciation for the broad range that exists, spanning technical and non-technical realms.

Next we discuss assets, in the spirit of what organizations need to protect. Again the interpretation is broad, spanning physical and logical assets: laptops, communication devices, intellectual property, brands, customer relationships, data, people, processes, et al. The intention is that this broad perspective will prepare students as their teams identify assets for the organization they are studying. We discuss asset valuation, which provides another useful link to business methods for doing this. Recognizing the value of organizational assets is a natural bridge to the possibility of transferring the risk of protecting these assets via cybersecurity insurance.

The identification and valuation of assets fits comfortably into another structuring framework. With Sun Tzu's *Art of War*, identifying assets contributes to the "knows himself" part of "One who knows the enemy and knows himself will not be endangered in a hundred engagements." [20, p.135] By continuing this model, to "know the enemy" leads us to identifying threats and assessing the extent to which an organization is vulnerable to them, thereby completing the CATV model. Discussions of threats and vulnerabilities provide opportunities to introduce a myriad of topics: threat intelligence, insider threats, personnel security, vulnerability assessment, penetration testing, auditing, and intrusion detection and prevention systems.

4.3 Second Leg in Pi: Cyber Brief – Deep Dive into a Cybersecurity Issue

The second probe in cybersecurity is for each student team to conduct a research and analysis study of a different cybersecurity topic. We want students to leave the class with this one detailed analysis experience to complement their broad higher-level understanding of cyber. And as each team delivers technical briefings to the rest of the class, all students will get exposure to several such detailed studies. All cyber brief presentation materials are takeaways for all students so they leave with a set of briefings on contemporary cybersecurity topics. Team peer evaluations of the briefings provide feedback toward improvement in the students' presentation skills.

As student teams come together, they may either propose topics or choose from a list. Recent topics have included government-private information sharing, vulnerability markets, "no more passwords", cloud security, cyberwar, security with IoT, secure re-design of the Internet, advanced persistent threat, smartphone backdoors for law enforcement, cyberinsurance, secure voting machines, breach prevention, security for SCADA systems, defense in depth for cyber, threat intelligence, and managed security services.

5. LESSONS AND RECOMMENDATIONS

Course offerings to date have spawned some lessons that can support continuous improvement:

- Build on what students already know

  We wanted to build scaffolding from their starting points: have students reflect on how much cybersecurity they are already familiar with. Students are "sys admins" for their laptops, with attendant responsibilities to manage upgrades, configure web browsers, load applications, change passwords, and install security software for basic hygiene of malware detection. From their experiences, students often know about cookies, web browser settings, wireless routers, identity theft, and the difference between http and https. In addition, students may have had personal experience with

their laptops being compromised or performance degraded due to malware.

Key for the cybersecurity course is to build from this knowledge and these experiences. Students' laptops have firewalls; how do they work? How are they configured? What are alternative ways to architect firewalls? Does your laptop use fingerprint recognition? Does your organization link your laptop and smartphone with one-time login codes? Students' answers can easily lead to fruitful discussions on biometrics and various means of multi-factor authentication. With the diversity of students in a class, we take advantage of those who have specialized knowledge: they may have worked in IT security or with a non-profit or government agency on security and privacy. Providing opportunities for students to share their experiences contributes highly to the overall learning of the class.

- Build-in continuous improvement

  Anticipate the need for change. Keep topic modules packaged tightly – such as in the 10-15 minute range – so they can be easily revised and re-sequenced. External course drivers such as new threats, technologies, laws, and regulations will motivate revisions. The pi-shaped course content structure provides a helpful separation of concerns. The horizontal bar can be enhanced as new frameworks and models are introduced and perceived to have value. New assessment schemes can be integrated into the first leg of the structure, and new critical cyber-related issues are prime candidates for new cyber brief topics.

- Focus on specific learning outcomes

  It's still a lot. Decide what is important. It's tempting to want students to attain extensive breadth and depth, but we deal with the reality of the course context. Focus tightly on the learning objectives. Recognize that that you cannot cover all that you may want, so decide explicitly on students' desired state of knowledge when they leave the course. Provide multiple pointers on how they can continue their education and learning.

We needed continual attention to help ensure that the sheer volume of possible topics did not lead to an uncomfortably crammed course.

- Build and leverage professional networks

  Students appreciate guest discussions and webinars with cybersecurity and business leaders. The guest spots should not be overdone but they provide welcome touch points into current practice. The humbling lesson has been that the same message has been better received when it came from a guest than from us, even with our prior industry and current consulting experience. We also benefited from industry colleagues, including some who are adjunct faculty members, asking them for their comments on the design of the course.

- Seek frequent feedback

  Ask for more student feedback than may be typical. At the start of the course, ask students about their expectations for the course and their learning. During the course, ask what's working and what's not. With cybersecurity so prominent in the news, it is important to understand what students expect and to be open about what is planned and what is feasible to accomplish in the course.

- Technology-related outcomes are feasible for business students

  Even if all business students cannot be assumed to have programming experience, don't shy away from introducing technical subjects. Cybersecurity has a fundamental technological core. But think through very precisely what the learning objectives are in the technological realm and pay special attention to coming up with effective ways to introduce the subjects and guide students so it is reasonable that they can attain those outcomes. Favor visualizations. Functional block diagrams of process flows and system architectures can be effective. Diagrams can help distinguish host-based and network-based IDSs. Selective simulations and product demos can help to explain how technologies work.

- Cybersecurity needs active learning

Some key cybersecurity methods and practices sound trivial until you try to apply them. Going over the steps in the risk management process leaves students wondering why we are stating the obvious – identify risks, assess them, etc. It is only when student teams try to use such methods in our cyber assess activity that the questions start: there is a realization that applying these methods to a real organization is not so straightforward. Teams need to wrestle with applying such methods to a particular organization that has ongoing operations and needs.

6. CONCLUSION

Cybersecurity is a business issue. Organizations need leaders who understand cybersecurity issues and challenges. Initiatives to enhance cybersecurity education should include useful sharing of experiences in designing and developing courses specifically for business students so that the most effective teaching and learning practices can be used.

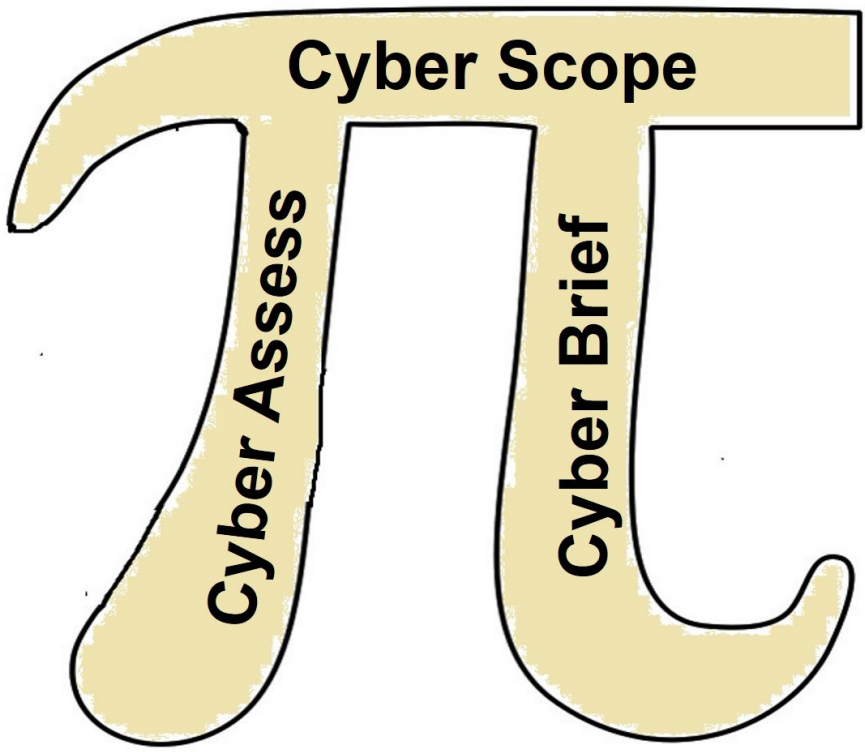

Figure 1. Pi-shaped Cybersecurity Course Structure

REFERENCES

[1] National Initiative for Cybersecurity Education (NICE), *National Cybersecurity Workforce Framework*, April 2013, http://csrc.nist.gov/nice/framework/.

[2] F. DeMeglio, "B-Schools Get into the Cybersecurity Business," *Bloomberg Business Week*, September 5, 2013, http://www.bloomberg.com/bw/articles/2013-09-05/b-schools-get-into-the-cybersecurity-business.

[3] K. Sheehy, "Information Security MBAs Teach Business Side of Cybersecurity," *US News & World Report*, February 21, 2012, http://www.usnews.com/education/best-graduate-schools/top-business-schools/articles/2012/02/21/information-security-mbas-teach-business-side-of-cybersecurity.

[4] The Second Principle, *Models for Teaching and Learning*, http://thesecondprinciple.com/teaching-essentials/models-teaching/.

[5] Canadian Underwriter, "New report gives Canada a 77% grade for cybersecurity readiness," November 20, 2015, http://www.canadianunderwriter.ca/news/new-report-gives-canada-a-77-grade-for-cybersecurity-readiness/1003908939/?&er=NA.

[6] National Council of ISACs, *Information Sharing and Analysis Centers*, https://www.isaccouncil.org/.

[7] A. Vorster and L. Labuschagne, "A Framework for Comparing Different Information Security Risk Analysis Methodologies," Proc. *South African Institute of Computer Scientists and Information Technologists*, SAICSIT '05, 2005, pp. 95-103.

[8] M. Viveros and D. Jarvis, *Cybersecurity Education for the Next Generation*, IBM Corporation, 2013, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&appname=CHQE_ED_ED_USEN&htmlfid=EDE12345USEN&attachment=EDE12345USEN.PDF.

[9] W. Agresti, "The four forces shaping cybersecurity," *IEEE Computer*, vol. 42, no. 2, pp. 101-104.

[10] J. McCumber, *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*, Boca Raton, FL: Auerbach Publications, 2004.

[11] D. Shoemaker and W. Conklin, Cybersecurity: *The Essential Body of Knowledge*, Boston: Course Technology, 2012.

[12] National Institute for Standards and Technology (NIST), *Cybersecurity Framework*, Version 1.0, February 2014, http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

[13] International Standards Organization, *Information Security Management*, ISO/IEC 27001, 2013, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

[14] National Institute for Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Rev. 4, April 2013, http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800-53r4_summary.pdf.

[15] J. Cebula and L. Young, "A Taxonomy of Operational Cyber Security Risks," Technical Note CMU/SEI-2010-Tn-028, December 2010.

[16] R. Anderson and T. Moore, The economics of information security, *Science*, vol. 314, 2006, pp. 610-613.

[17] C. Pfleeger, "Lessons Learned: Security is Inevitable," *IEEE Security & Privacy*, vol. 13, no. 6, 2015, pp.22-28.

[18] J. Saltzer and M. Schroeder, "The Protection of Information in Computer Systems," *Proc. IEEE*, vol. 63, no. 9, 1975, pp. 1278-1308.

[19] SANS Institute, *Controls for Effective Cyber Defense*, 2015, https://www.sans.org/critical-security-controls.

[20] S. Tzu, *The Art of War*, Translation by R. Sawyer, New York: Barnes & Noble, 1994.