Direct From the Practitioner

Crowdsourcing for Cybersecurity Curriculum

Cybersecurity threats and the technology to deal with them are constantly evolving. Because of this, both aspiring and current cybersecurity practitioners must be educated about relevant issues and should keep up to date on new developments so they can adapt and excel in defending their enterprises' assets. Although it can be difficult, there are many ways that institutions of higher education, technical training institutions and other learning-focused entities can determine relevant cybersecurity course content to offer their students and members.

Determining Relevant Course Content

A few approaches are available when tackling the task of curriculum development. In universities and technical training institutions, the most common approach is to form a curriculum or advisory committee composed of dedicated teaching faculty and, perhaps, practicing industry professionals. For example, when tasked with creating a new graduate-level cybersecurity management course, one university's curriculum committee had to determine which topics were truly relevant for the students taking the course, who would then enter the cybersecurity workforce. Likewise, in organizations such as ISACA®, (ISC)[2] and the International Council of Electronic Commerce Consultants (EC-Council), practicing members who hold specific certifications may be asked to convene in a workshop environment to carry out a similar task. However, curriculum committees and workshops can be hard to manage due to the members' different schedules, priorities and interests.[1] Because of this, committees and workshops tend to have a limited number of contributors, which can lead to a lack of professional diversity, ideas and inputs.[2, 3]

That being said, the combination of the curriculum committee's decision-making process and practitioners' knowledge and experience was a great basis for developing a relevant cybersecurity curriculum for the university course in question. Input from a larger population of cybersecurity practitioners and leaders was needed. This led to the idea of using crowdsourcing to develop the curriculum.

Crowdsourcing for Curriculum Development

Prior to crowdsourcing for curriculum topics, the course developer created a list of predetermined topics that might be important for students taking the course. These topics were then formatted into a

Brian K. Ngac, CRISC, CISM, CGEIT, CCISO, CISSP-ISSAP, ISSEP, ISSMP, PMP
Is an instructor of information systems and operations management at George Mason University's School of Business (Fairfax, Virginia, USA). He also teaches in the school's executive master's program in technology management. His research interests include cybersecurity executive management, the human factor in cybersecurity implementation and cybersecurity education.

> "CROWDSOURCING CONFIRMED THAT MOST OF THE PREDETERMINED TOPICS WERE RELEVANT AND IMPORTANT TO CYBERSECURITY PROFESSIONALS."

Google Forms questionnaire that was sent to 50 potential participants chosen from the course developer's network on LinkedIn. Those 50 participants were encouraged to forward the questionnaire to other people in their networks. The questionnaire asked participants to select all the predetermined topics they considered important for students taking the course (**figure 1**)—that is, those that would permit them to hit the ground running and excel in the workplace. Participants were encouraged to submit additional topics of importance for graduates entering the cybersecurity field (**figure 2**). The questionnaire also asked participants about their professional backgrounds, such as industry, position and years of experience in the cybersecurity field.

After two weeks, the survey was closed, and data aggregation began. First, professional demographics were used to filter out respondents who were not cybersecurity practitioners. That left 18 respondents, which exceeds the number of members on a typical curriculum committee. Second, participants' votes for each predetermined topic were counted, and the topics were classified (**figure 3**):

- Topics with 15 or more votes were considered a high priority (white)
- Topics with 10 or fewer votes were classified as lower priority (red)
- Remaining topics were classified as medium priority (yellow)

Figure 1—Question to Confirm Important Identified Topics

2 Which of the following would you consider important topics that a cybermanagement professional needs to learn and understand for managing information security with vendors and partners?

Check all that are applicable.

- ☐ Building, Buying and Outsourcing—Introduction of Security Consideration
- ☐ Security Considerations With Partners, Teammates and Subsidiaries
- ☐ Supply Chain Security Management (The Theory)
- ☐ IT Acquisition Security Management (The Practice/Process)
- ☐ Third-Party Threats and Security Management
- ☐ Managing Security With Cloud Service Providers (CSPs)
- ☐ Managed Security Service Providers (MSSPs)
- ☐ Mergers and Acquisition Security Considerations
- ☐ Security Considerations While Downsizing
- ☐ Business Continuity
- ☐ None of These Are Important

Figure 2—Question to Suggest Additional Relevant Topics

7 Optional Additional Topics #5: In addition to the topics listed above in the second question, what do you feel is another important topic a cybermanagement professional should learn and understand when managing information security with vendors and partners? Please list one below. If you have more than one for this last optional question, you can separate each key skill with a semicolon (;).

Figure 3—Classification of Predetermined Topics

Building, Buying and Outsourcing—Introduction of Security Considerations
Security Considerations With Partners, Teammates and Subsidiaries
Supply Chain Security Management (The Theory)
IT Acquisition Security Management (The Practice/Process)
Third-Party Threats and Security Management
Managing Security With Cloud Service Providers (CSPs)
Managed Security Service Providers (MSSPs)
Mergers and Acquisition Security Considerations
Security Considerations While Downsizing
Business Continuity

Benefits of Crowdsourcing

The aggregated crowdsourced data yielded a few benefits for the course developer. First and foremost, crowdsourcing confirmed that most of the predetermined topics were relevant and important to cybersecurity professionals. The data aggregation also suggested which topics were less important. As a result, the course developer integrated lower-priority topics (red in **figure 3**) into the high-priority topics (white in **figure 3**). For example, the topic of managed security service providers (MSSPs) could be incorporated into the discussion of cloud service providers (CSPs), and security considerations while downsizing could be covered during discussions of security considerations related to mergers and acquisitions.

Second, the 18 respondents suggested a total of 73 additional topics. As a result, the course developer determined that a new topic should be introduced to the curriculum: contract, legal and regulatory considerations. Thirteen of the respondents had suggested a similar topic.

A third benefit was realized when the course developer noticed that many of the additional topics suggested by the respondents could be categorized as subtopics under the predetermined topics. Even though the participants were not asked to suggest subtopics, their suggestions were inadvertently helpful to the course developer in defining sections for each topic's lecture. **Figure 4** shows a sample of the suggested topics and how the course developer categorized each one as a subtopic under an existing predetermined topic.

Another benefit that arose from this crowdsourcing effort was the interest shown by respondents in teaching at the university or giving guest lectures. When students get firsthand information from those on the front lines, it makes them more engaged in the topic.[4] In addition to obtaining relevant input from working cyberpractitioners, crowdsourcing can put educational institutions in contact with those who may be interested in teaching and sharing their knowledge.

Of course, this method of collective curriculum development and enhancement through the use of crowdsourcing can be applied to other fields of study, such as auditing. And, although this particular crowdsourcing effort was aimed at a university's graduate-level cybersecurity course,

"EVEN THOUGH THE PARTICIPANTS WERE NOT ASKED TO SUGGEST SUBTOPICS, THEIR SUGGESTIONS WERE INADVERTENTLY HELPFUL TO THE COURSE DEVELOPER IN DEFINING SECTIONS FOR EACH TOPIC'S LECTURE."

Figure 4—Example of Suggested Topics and Their Categorization

Suggested Topics	Classify/Categorize	Current Topic
The particular security needs of that partner, who may not know themselves (e.g., HIPAA, FERPA)	Current Topic: Subtopic	Security Considerations With Partners Teammates Subsidiaries
Cyberresilience	Current Topic: Subtopic	Business Continuity
Supply chain risk management (the practice/process)	Current Topic: Subtopic	Supply Chain Security Management (The Theory)
Third-party risk	Current Topic: Subtopic	Third-Party Threats and Security Management
Separating IT vendors/partners from other business vendors/partners	Current Topic: Subtopic	Security Considerations With Partners, Teammates Subsidiaries
Vendor life cycle (i.e., due diligence, contracting, monitor/assess/manage, offboard)	Current Topic: Subtopic	IT Acquisition Security Management (The Practice/ Process)
Practical implementation issues using real-world examples	Current Topic: Subtopic	Mergers and Acquisition Security Considerations
Vetting vendors and contractors, etc.	Current Topic: Subtopic	Security Considerations With Partners, Teammates Subsidiaries
Maintenance and/or obsolescence of COTS	Current Topic: Subtopic	Building, Buying and Outsourcing—Introduction of Security Considerations
If a partner's nontechnical team does not understand the importance of security procedures (explained in layman's language), they may push to cut corners. It is important that the professional listen to their business concerns and explain clearly why certain security considerations are required.	Current Topic: Subtopic	Security Considerations With Partners, Teammates Subsidiaries
Supplier outreach	Current Topic: Subtopic	IT Acquisition Security Management (The Practice/ Process)
Security of software systems' supply chain or value chain	Current Topic: Subtopic	Supply Chain Security Management (The Theory)
Vendor SOC 1/2/3, ISO 27001 cert. Meaning and limitations, considerations for chained audit	Current Topic: Subtopic	Third-Party Threats and Security Management
Security considerations for outsourced software/systems development	Current Topic: Subtopic	Building, Buying and Outsourcing—Introduction of Security Considerations

other educational institutions can adopt similar methods. For example, many practitioners have been asked to attend professional certification workshops to update the content of examinations and related training seminars. The crowdsourcing method can be used to reach a wider audience, such as individuals who may be unable to travel for whatever reason (e.g., COVID-19) but still need continuing professional education (CPE) hours. Since October 2020, a large US organization employing more than 16,000 people has been using crowdsourcing to determine important and relevant topics for its new management development training program. The program will be used to train current employees who aspire to become managers and new managers hired by the organization.

Hurdles Inherent in Crowdsourcing

The first challenge in crowdsourcing is getting responses. In this case, the course developer sent direct messages to approximately 50 connections on LinkedIn but received only 14 responses; the other four responses came from individuals in the original connections' networks. Although a typical curriculum committee has fewer than 18 members, it would have been valuable to have a higher response rate and, possibly, a more diverse group of respondents.

The second challenge is determining which respondents are providing "good" inputs. In this case, even though the questionnaire requested information about each participant's professional background for filtering purposes, some of the inputs suggested that the respondent's expertise was in a different niche of cybersecurity.

The third challenge is that it is very time consuming to analyze unstructured data—specifically, the participants' suggested additional topics. It took the course developer about three hours to go through all the suggested topics and categorize them, even though there were only 18 participants and 73 additional topics. Research into automating the categorization of this type of crowdsourcing data would be useful, and it is happening.

Conclusion

As the cyberthreat environment changes and evolves, cybersecurity education must also evolve. Cybersecurity curriculum must be based on best practices and include hands-on activities. It must also be relevant so students can immediately apply their knowledge in the field. By utilizing crowdsourcing, a course developer can identify relevant topics and subtopics for a new course or update an existing one. And for enterprises with the ability to reach thousands to hundreds of thousands of potential participants, the benefits of crowdsourcing are endless. Crowdsourcing can not only produce a more diverse set of relevant topics but also mitigate many of the challenges of depending on committees and workshops to develop and update curriculum. Moreover, a cybersecurity curriculum that is updated and relevant provides cybersecurity professionals, managers and leaders with the information and knowledge they need to be successful in protecting their organization's assets and consumers, themselves and the people they care about protecting.

"CROWDSOURCING CAN NOT ONLY PRODUCE A MORE DIVERSE SET OF RELEVANT TOPICS BUT ALSO MITIGATE MANY OF THE CHALLENGES OF DEPENDING ON COMMITTEES AND WORKSHOPS TO DEVELOP AND UPDATE CURRICULUM."

Author's Note

Effective crowdsourcing for the development of cybersecurity curriculum requires an experienced crowd that cares about training tomorrow's cyberwarriors. All cybersecurity practitioners, managers, executives and leaders are encouraged to join the Cybersecurity Management Curriculum Development LinkedIn group at *https://www.linkedin.com/groups/8942263/*.

Endnotes

1 Lu, J.; "The Role of Advisory Committees in Universities," *Journal of Teaching in Travel and Tourism*, vol. 4, iss. 4, 2004, p. 47–54
2 Mathew, L.; B. B. Brewer; J. D. Crist; R. J. Poedel; "Designing a Virtual Simulation Case for Cultural Competence Using a Community-Based Participatory Research Approach: A Puerto Rican Case," *Nurse Educator,* vol. 42, iss. 4, 2017, p. 191–194
3 Satterfield, J. M.; S. R. Adler; H. C. Chen; K. E. Hauer; R. Salazar; "Creating an Ideal Social and Behavioural Sciences Curriculum for Medical Students," *Medical Education,* vol. 44, iss. 12, 2010, p. 1194–1202
4 Ngac, B.; "Cyber Professionals Can Be the Best Cyber Teachers," *ISSA Journal*, February 2020, p. 30–33, *https://mydigitalpublication.com/publication/?m=1336&i=649364&p=30*