STUDENT LEARNING ASSESSMENT REPORT

PROGRAM: MS Cybersecurity
SUBMITTED BY: Michelle Liu
DATE: September 30, 2020

Executive Summary: Description of Assessment Process

List *all* of the program's learning outcomes, as of the assessment year's catalog: *(regardless of whether or not they are being assessed this year)*

Learning Outcome	Year of Last Assessment	Assessed This Year *(Y=Yes)*	Year of Next Planned Assessment
Identify and solve cybersecurity issues in business and society by managing cybersecurity operations using available tools and techniques	2017-2018	Yes	2020-2021
Review and understand the legal, regulatory, policy, and ethical issues related to securing cyberspace and ensuring the privacy of personally identifiable information (PII)	2015-2016		2020-2021
Communicate effectively with others, including technologists and managers in cybersecurity and IT as well as users and managers in the business context	2018-2019		2020-2021
Use specialized knowledge to continue to update skills and obtain, if applicable, certifications in the cybersecurity field	2017-2018	Yes	2020-2021
Optimize the effectiveness of cybersecurity in an organization by performing vulnerability assessments, risk mitigation, auditing, and certification and accreditation of information systems	2017-2018		2020-2021
Work effectively as a member or as a leader of a cross-disciplinary team in the cybersecurity field where teamwork is essential to the success of a time-critical project	2018-2019		2020-2021
Develop the knowledge and skills required to pursue lifelong learning in areas relating to cybersecurity and to adapt to an ever-changing global technological and business environment through information literacy activities relevant to a fast-changing discipline	2018-2019		2020-2021

Provide a <u>brief</u> description of the assessment process used including how results are shared and discussed and strengths, challenges, and planned improvements to the <u>process</u>, providing evidence of a culture of continuous improvement based on assessment. If there is something that is impeding your ability to implement improvements, please comment on those issues *(generally not more than two paragraphs, may use bullet points)***:**

In 2019-20, the assessment process was effective and cybersecurity faculty responded well to all calls for data (full-time and part-time). The overall outcome assessment strategy and the specific outcome assessment techniques were discussed early in the school year at a department meeting of cybersecurity full-time faculty. Based on these discussions, the chair and the program director met individual adjunct faculty who were involved in providing data for the various assessment techniques. The results from the previous assessment were discussed along with this year's cybersecurity assessment plans. A plan was put in place to focus on the two learning outcomes being assessed in the designated courses. Outcomes and their measurement for the 2018-19 outcomes assessment were discussed and data collection requirements were identified. A graduate student was designated as the data collection point of contact and worked closely with the chair to ensure the faculty provided the necessary data in a timely manner. The major data and documents used to generate this report are stored in the Canvas courses for 2019-20, Box, and MU Plan.

A number of previously identified initiatives were also refined, implemented, and extended as part of our continuous improvement process including the need for reexamine the course sequencing and reducing some prerequisites for the certain elective courses and specialty courses, revising scheduling to meet the additional number of students, and the development of specialties in cyberintelligence.

Closing the Loop: Progress on Planned Improvements from Prior Year

Describe how the program implemented its planned improvements from last year:

Outcome	Planned Improvement	Update
Communicate effectively with others, including technologists and managers in the cybersecurity, IT, and users and managers in the business context	The program director will work with instructors to instigate a more formal draft and review process for the master thesis project process to enable students to be more prepared in both writing and oral skills. The department will also organize and host at least one department-level workshop focusing on IT/Cybersecurity in which master students will present their thesis work in the 19/FA-20/SP academic year.	The cybersecurity faculty discussed writing across the curriculum both informally as a small group and formally at a couple of departmental meetings held in AY 2019-20. It was seen as a common issue across all classes. A library of writing materials was developed as a resource for students and students were encouraged to use the CTL writing tutoring service as well as use Brainfuse, a writing tutor service program integrated in Canvas.
Work effectively as a member or as a leader of a cross-disciplinary team in the cybersecurity field where teamwork is essential to the success of a time-critical project	We have been investigating online group techniques at the department level. In addition, the director will work with instructors to reexamine and renovate some group-based projects that are assigned in online courses so that the projects are more suitable for online courses.	Both the program directors and the department chair researched on several different online group techniques and the final results were shared during the department meetings and the department internal portal. The chair also meets each faculty who teaches online courses, going through some of the findings and those faculty are starting to teach using those techniques in their online courses. For example, several faculty members have implemented different online group techniques and tools such as Zoom, Padlet, Panopto, Google Hangout to host synchronous, virtual lectures, discussions, and office hours for their online classes. Students learn those techniques by participating in those activities and group projects.
Develop the knowledge and skills required to pursue life-long learning, in areas relating to cybersecurity and to adapt to an ever-changing, global technological and business environment through information literacy	Involvement of library services in the various classes is spotty (some students get the presentation 2 or 3 times) and so we are working with the library liaison to improve coverage over the program, focusing on specific assignments in each class.	The library liaison has complied and curated the library resources based on the program (IT and cybersecurity). The library resources links now also have been integrated in our Canvas site and students can access the program specific, library resources from each Canvas course website.

Outcome	Planned Improvement	Update
activities relevant to a fast-changing discipline		

Provide a response to last year's University Assessment Committee review of the program's learning assessment report:
Comment:
The University Assessment Committee made no recommendations for the next assessment process.
Response:
The MS, Cybersecurity program will continue its work in the learning assessment process.

Outcomes Assessment 2019-2020

Learning Outcome 1: Identify and solve cybersecurity issues in business and society by managing cybersecurity operations using available tools and techniques

Outcome Measures *Explain how student learning will be measured and indicate whether it is direct or indirect.*	**Performance Standard** *Define the acceptable level of student performance.*	**Data Collection** *Discuss the process for collecting this data: who conducted the assessment, when, and how?*	**Result** *Did you meet your target? What was the result?*
Direct: Use of effective cybersecurity best practices to defend a system cyberattack in the capstone course, IT670, Cybersecurity, Attack and Defend	75% of students are able to analyze an attack scenario, successfully defend and effectively document findings and recommend solutions in IT670 and provide an adequate response (4 or more) on a scale of 0 (no response) to 5 (excellent). (See Rubric 1)	The assignments were collected from Canvas for the Fall 2019 semester (20 students) and spring 2020 (25 students). The assignments were downloaded from Canvas before they were graded by the professor.	The responses were reviewed by a panel of three professors: the Chair, the program director, and one full-time faculty, all experts in the field of cybersecurity. Each panel member was given an opportunity to rate the solutions for their adherence to best practices in the field (0 through 5). 32 of the 45 students (approximately 71%) obtained an average of 4 or more on the rubric. The standard was met.
Direct: Development of an effective policy document as part of the final project in IT570, Cybersecurity: Law, Policy and Compliance.	75% of all students generate an effective policy in response to a class final project which focuses on managing cybersecurity operations (a grade of 21 as the maximum score on the Rubric 2)	The assignments were collected from Canvas for the Fall 2019 (32 students) and spring 2020 semester (18 students). The assignments for 50 students were downloaded before they were graded by the professor.	The responses were reviewed by an adjunct from the Federal government and two full-time faculty members, both experts in cybersecurity, and rated according to a rubric (see Rubric 2). 43 of the 50 students achieved 80% or more on the rubric (approximately 85%). **The standard was met.**
Indirect: From the 2019 Alumni Data from PIE: responses to the question: confidence that the student can "solve problems in	80% of students should feel good or adequate about their response to the question "solve problems in	Data was to be collected from the 2019 Alumni Survey,	There were 7 responses to the survey.

Outcome Measures *Explain how student learning will be measured and indicate whether it is direct or indirect.*	Performance Standard *Define the acceptable level of student performance.*	Data Collection *Discuss the process for collecting this data: who conducted the assessment, when, and how?*	Result *Did you meet your target? What was the result?*
your field using your knowledge and skills"	your field using your knowledge and skills"	conducted by the Office of Institutional Effectiveness	100% of all the graduating students answered good or excellent **The outcome was met.**

Interpretation of Results

Analysis and Implications: *What does this result tell you about the extent to which your students achieved this outcome? What are the strengths and weaknesses that this result highlights, and what are the implications for your curriculum or your program?*

Two of the three outcome measures were met. The first measure on cybersecurity attack and defense capability was not met. IT670 has been regarded as one of the most technical courses in the program by the students. As many students joining our cybersecurity program are career changers with a fairly diverse background ranging from criminal justice to psychology to statistics, IT670 is especially challenging due to its hands-on, technical nature.

Discuss planned curricular or program improvements for this year based on assessment of outcome:

We took this situation into consideration and decided to provide an alternative course for the students who are career changers and would not be working as penetration tester or in a technical position in the cybersecurity field when they graduate from the program. We are piloting to offer both IT670 and IT566 (Data Visualization) in the spring 2020 so that those who do not want to go to the technical route have the option to take IT566. We will closely track the students who take IT566 as the alternative of IT670 and gain their feedback during the semester and after the semester ends. Based on the feedback, we will adjust the curriculum and may make this structure permanent in the degree plan.

Learning Outcome 2: Use specialized knowledge to continue to update skills and obtain, if applicable, certifications in the cybersecurity field

Outcome Measures	Performance Standard	Data Collection	Result
Direct: Performance on the final online assessment in IT535, Advanced Computer Security, whose knowledge base is the same as the CISSP certification requirements, the premier certification in the cybersecurity field	70% of the students will achieve a score of 70% or more on the final certification readiness test in the course (70% is the passing rate for the official examination)	Tests are automatically scored and results are downloaded from Blackboard	20 students enrolled in Fall 2019 and 21 students enrolled in Spring 2020. 28 out of 41 achieved the 70% level in the certification test (68% of the total enrollment). **The standard was not met**
Direct: Students felt comfortable or very comfortable in their ability to pass the CISSP exam after finishing IT535, Advanced Computer Security	70% of students were comfortable in their ability to pass the CISSP certification test.	The topic will be discussed on the discussion board, with students not being able to see the other submissions	The responses on the discussion board were evaluated and 35 of the 41 students (86%) expressed confidence that the course material prepared them for the knowledge required to pass the certification exam, however only 20 felt they would pass the exam at that

Outcome Measures	Performance Standard	Data Collection	Result
		until they had entered their response.	point, because of the lack of study time. **This standard was met.**
Indirect: From departmental survey given to graduating students, the number of students who have earned, or will earn, at least one industry cybersecurity certification, including CEH, CSX, or CISSP	60% of graduating students left with at least one industry certification on graduation from Marymount or intended to take them in the next 90 days	Data collected from the departmental survey conducted before graduation.	Eight out of sixteen responses stated that they had taken and passed the CISSP exams and another four said that they had scheduled the test (75%). **The standard was met.**

Interpretation of Results

Analysis and Implications: *What does this result tell you about the extent to which your students achieved this outcome? What are the strengths and weaknesses that this result highlights, and what are the implications for your curriculum or your program?*

Two of the three factors were met. IT535 covers the essential components of the CISSP certification exams, one of the most prestigious as well as challenging certification exam in the IT and cybersecurity field. Later courses reinforce the concepts covered and confidence seemed to increase as the students progressed through the program.

Discuss planned curricular or program improvements for this year based on assessment of outcome:

We will continue to offer some certification training workshops or bootcamps for our students. AWS architecture certificate and CSSIP bootcamp training are two examples. We will also bring in different guest speakers (with the CISSP certification) to share the experiences and resources for preparing the certification exams in different courses offered in the program.

Appendices *(please only include items that will help reviewers understand your process – for example, test questions, rubrics, survey questions, more detailed description of assessment measures, summary tables of survey results, etc.)*

Rubrics

Rubric 1: Evaluation of Web Application Attack and Defend Assignment

Attribute	Measure	Scoring	Student Score
Review the completion of each individual task looking for evidence that the student was able to apply the knowledge of common web app vulnerabilities to the virtual lab scenarios	Grade as fully completed, mostly completed, partially completed with relevant knowledge present, or partially competed with little knowledge present, barely completed, and incomplete	5, 4, 3, 2, 1 and 0	
Review the screenshots to look for evidence of applying the knowledge of web app attack countermeasures to defend the system	Mark as Outstanding, Adequate, Above Average, Average, Below Average, and	5, 4, 3, 2, 1 and 0	
Review the written report for readability and technical analysis capability	Mark as well developed documentation, satisfactorily developed documentation, or inadequate or missing	5, 4, 3, 2, 1 and 0	
Total score	Calculate score	Students receiving a score of 0 through 15.	

Rubric 2: Evaluation of Cybersecurity Policy in IT570, Cybersecurity: Law, Policy and Compliance Requirements Engineering

Attribute	*Measure*	*Scoring*	*Student Score*
Rate the complexity of the topic selected for the policy document and its applicability to today's cybersecurity environment	Evaluate and score as follows: excellent, advanced, good, basic, poor, or no submission	5, 4,3,2,1, and 0	
Rate the depth of coverage of the policy in the report	Evaluate and score as follows: extensive coverage, good coverage, adequate coverage, limited coverage, poor coverage, and no coverage	5,4,3,2,1, and 0	
Review the form and format of the document to ensure the quality and clarity of the policy document	Evaluate and score as follows: effectively organized, organized, poorly organized, or no submission	3,2,1, and 0	
Evaluate the language used in the report and its ability to be understood by its audience, the average user in the organization	Evaluate and score as follows: well written (no jargon or jargon explained), adequately written (jargon mainly explained), includes some jargon, and full of jargon, and no submission	4,3,2,1, and 0	
Evaluate the report with respect to best practice policy standards	Excellent conformance,, good conformance, average conformance,, below par conformance, and no conformance	4, 3, 2, 1, and 00	
Total score	Calculate score	Scores from 0 through 21	