STUDENT LEARNING ASSESSMENT REPORT

PROGRAM: Cybersecurity (MS)
SUBMITTED BY: Michelle Liu
DATE: August 30, 2018
BRIEFLY DESCRIBE WHERE AND HOW ARE DATA AND DOCUMENTS USED TO GENERATE THIS REPORT BEING STORED: CANVAS COURSES FOR 2017-18, BOX, AND MU PLAN

EXECUTIVE SUMMARY

Program description from the Course Catalog: Please copy and paste the current year's catalog description of this program. This is generally a one-two paragraph description immediately following the name of the program. Please be sure to include the listing of program outcomes as printed.

Marymount University is designated as a National Center for Academic Excellence for Cyber Defense (CAE/CD) by the National Security Agency and the Department of Homeland Security through 2020. In addition, Marymount students enrolled in this program are eligible to compete for the National Science Foundation's Cybercorps Scholarship for Service program.

Marymount's cybersecurity program is designed to prepare individuals for high-level positions in computer and information security by developing the necessary knowledge, skills, and abilities in the technology and management of cybersecurity. Graduates will work in the protection of the digital world for the federal government, state and local governments, nonprofits, and industry.

Students may pursue a dual degree in cybersecurity and information technology to broaden their knowledge in cybersecurity management and leadership.

Because of the university's proximity to federal agencies, including the Department of Homeland Security, Department of Defense, and National Science Foundation, faculty members in the program are involved in and aware of current federal government initiatives and requirements. Further, program leaders are able to call on practitioners in the field as guest speakers and adjunct professors.

This 36-credit program is offered in online and face-to-face formats. Courses are rigorous, including readings, collaboration, and practical assignments using inquiry-based learning techniques with online multimedia presentations, online tools, and online simulations and labs. The program is designed to prepare individuals for promotion to a cybersecurity analysis position, and to meet the certification requirements currently imposed on the profession, particularly by the Department of Defense. While all other coursework may be completed online, the culminating course is completed in residency in order to take advantage of the cybersecurity resources of the Washington, DC, area. Students will gain hands-on practice with equipment and tools, interacting with cybersecurity experts in government and industry.

The program is committed to exhibiting the highest professional and ethical standards addressing the needs of working individuals, full-time students, and business and government organizations. A variety of electives enable individual students to tailor the program to their knowledge base and career aspirations.

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

Learning Outcome	Year of Last Assessment	Assessed This Year	Year of Next Planned Assessment
1. Identify and solve cybersecurity issues in business and society by managing cybersecurity operations using available tools and techniques	2014-15	X	2019-20
2. Review and understand the legal, regulatory, policy, and ethical issues related to securing cyberspace and ensuring the privacy of personally identifiable information (PII)	2015-16		2020-21
3. Communicate effectively with others, including technologists and managers in the cybersecurity, IT, and users and managers in the business context	2013-14		2018-19
4. Use specialized knowledge and techniques to obtain skills and, if applicable, certifications in the cybersecurity field	2014-15	X	2019-20
5. Optimize the effectiveness of cybersecurity in an organization by performing vulnerability assessments, risk mitigation, forensic analysis, auditing, certification and accreditation of information systems	2014-15	X	2019-20
6. 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	2015-16		2018-19
7. 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 activities relevant to a fast-changing discipline	2015-16		2018-19

Describe <u>briefly</u> how the program's outcomes support Marymount's mission, strategic plan, and relevant school plan *(generally not more than two paragraphs, may use bullet points)*:

The MS in Cybersecurity program fully supports the graduate education mission of Marymount University and the outcomes include both the opportunity to acquire a high level of competency in the cybersecurity domain (e.g., identify and solve cybersecurity issues in business and society) and to gain experience in the application of advanced knowledge and skills (including management, leadership, policy development, compliance, and technical competence). Furthermore, the program's outcomes align with Marymount's strategic plan and vision by fostering academic excellence as well as promoting community engagement. The statement is corroborated by the following practices in the program:

- Inquiry learning is a key in the program and all professors (full-time and part-time) are encouraged to use activities and labs, in-classroom or as homework assignments, to reinforce the subject-matter learning in the classroom. These activities may occur through individual and group assignments.
- The program ensures a personalized education through small classes and faculty/student collaboration. Cybersecurity graduate classes have averaged around 16 students, large enough to have a variety of opinions and experiences on the discussion board, but small enough to allow for individual attention and extensive faculty/student collaboration for the lab work and other activities. Note: some of these courses are also taken by IT graduate students who are in dual degree programs in IT/Cybersecurity specializing in the cybersecurity domain.
- Ethics are an integral part of each course but particularly emphasized in the required course IT570, Cybersecurity: Law, Policy, Ethics, and Compliance. Cross-disciplinary collaboration occurs in the early courses such as IT530, Computer Security, and this includes students from other programs including MSIT, and the MSHCM/MSIT and MBA/MSIT dual degree programs.

- The program reinforces community engagement by using DC-area resources and new technologies to enhance the global perspective of the Marymount community. Marymount is surrounded by operational cybersecurity locations, such as the Department of Homeland Security and the CIA We make also use of the DC area as a center of cybersecurity expertise for adjuncts, for frequent guest speakers and for members of our Cybersecurity Roundtable. The Cyber Center offers several events including individuals from the local cybersecurity community as speakers or members of panels. Marymount faculty also participated in many cybersecurity events in the area, promoting the program.
- The program provides various opportunities across the curricula for students' growth in both academia and career aspects. The program has sustained a steadily growth during the past five years and we are going to start our DSc program in Cybersecurity in the Fall 2018. For the 2017-18 academic year, there were 78 students in Fall 2017, 85 in Spring 2018, and 52 in summer 2018 semester. Most of these students are working professionals, mainly in networking or information security, who are looking to raise their skills, knowledge, and promotion prospects in the growing field of cybersecurity.

Provide a <u>brief</u> description of the assessment process used including strengths, challenges and planned improvements to the process, and provide evidence of the existence of a culture of continuous improvement based on assessment *(generally not more than two paragraphs, may use bullet points)***:**

In 2017-18, 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 three learning outcomes being assessed in the designated courses. Outcomes and their measurement for the 2015-16 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.

A number of other initiatives were also identified as part of our continuous improvement process including the need for an "internship" program, revising scheduling to meet the additional number of students, the development of specialties in healthcare security, cyberintelligence, and data science.

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

Outcome	**Planned Improvement**	**Update** *(Indicate when, where, and how planned improvement was completed. If planned improvement was not completed, please provide explanation.)*
Review and understand the legal, regulatory, policy, and ethical issues related to securing cyberspace and ensuring the privacy of personally identifiable information (PII)	While cybersecurity laws are slow to change at the Federal level, there are many state and local changes as well as those that are specific to a particular industry. In addition, organizations such as NIST are continuously producing new and revised policy documents. Staying up-to-date for faculty and students is important. For example, NIST just released guidance on the	The program director has worked closely with the department chair as well as faculty members to set up the internal department portal to disseminate the government reports on legal and regulatory development in the cybersecurity related field, share the latest updates of NIST publications on security

Outcome	Planned Improvement	Update *(Indicate when, where, and how planned improvement was completed. If planned improvement was not completed, please provide explanation.)*
	security of the Internet of Things which was distributed to the appropriate faculty. This process will be systematized. We plan for one of the graduate assistants to maintain a spreadsheet that includes all current changes, together with links to the documents and discussion of the impact of these changes, and to distribute this to our cybersecurity faculty on a regular basis.	policies and measures, and the information on webinars hosted by the industry leaders and federal agencies on such topics. In addition, a Slack group has been set up to facilitate such communications and collaborations. For example, GDPR and its impacts on companies handling and storing personal data have been raised and discussed among faculty members through the portal. All of the above practices equip our faculty with up-to-date knowledge of the legal, ethical, policy and privacy related issues and development in the field so that they can impart and discuss such knowledge in class.
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 are investigating online group techniques and when the research is complete we will distribute to the relevant faculty.	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 WebEx, Canvas Conference and 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 activities relevant to a fast-changing discipline	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.

Provide a response to last year's University Assessment Committee review of the program's learning assessment report:

Note: No assessment report was submitted during 2016-17 because a five-year program review was conducted during that period.

Outcomes Assessment 2017-2018

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

Assessment Activity

Outcome Measures *Explain how student learning will be measured and indicate whether it is direct or indirect.*	**Performance Standard** *Define and explain acceptable level of student performance.*	**Data Collection** *Discuss how the data was collected and describe the student population*	**Analysis** *1) Describe the analysis process. 2) Present the findings of the analysis including the numbers participating and deemed acceptable.*
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).	The assignments were collected from Canvas for the Fall 2017 semester (12 students) and spring 2018 (10 students). The assignments were downloaded from Canvas before they were graded by the professor.	The responses were reviewed by a panel of four professors: the Chair, the program director, one full-time faculty, and one adjunct 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). 19 of the 22 students (86.4%) 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)	The assignments were collected from Canvas for the spring 2018 semester The assignments for 23 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 1). 19 of the 23 students achieved 80% or more on the rubric (82%), with 4 have 21, the highest possible score. The standard was met.
Indirect: From the Graduating Student Survey, confidence that the student can "solve problems in your field using your knowledge and skills"	80% of students should feel good or adequate about their response to the question "solve problems in your field using your knowledge and skills"	Data was to be collected from the 2017-18 Graduating Student Survey, conducted by the Office of Institutional Effectiveness	Only 2 students responded to the survey. One rated good and the second rated excellent to this question. It is not possible to draw and conclusions from this small sample.

Interpretation of Results

Describe the extent to which this learning outcome has been achieved by students *(Use both direct and indirect measure results)***:**

The standard was met by both of the direct measures, the third measure did not have enough responses to draw and conclusions.

Briefly describe program strengths and opportunities for improvement relative to assessment of outcome:

Both of the direct measures were based on the use of active learning techniques and involved the students doing work that they would expect to do in the government workspace. Both of these courses were conducted in the classroom, we now need to evaluate active learning in some of the online courses.

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

We will continue to expose students to best practices in the cybersecurity field and to ensure students can apply their knowledge in the workplace.

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

Assessment Activity

Outcome Measures *Explain how student learning will be measured and indicate whether it is direct or indirect.*	**Performance Standard** *Define and explain acceptable level of student performance.*	**Data Collection** *Discuss how the data was collected and describe the student population*	**Analysis** *1) Describe the analysis process. 2) Present the findings of the analysis including the numbers participating and deemed acceptable.*
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	10 of the 16 students in 14/Fall achieved the 70% level in the certification test and 9 of the 12 students in 15/Summer (Total 19 of 28 - 68%). The standard was not met
Direct: Students felt comfortable or very comfortable in their ability to pass the CISP 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 until they had entered their response.	The responses on the discussion board were evaluated and 24 of the 28 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 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.	4 students graduated in Fall 2014 and 4 graduated in spring/summer 2015. Each student was interviewed as they graduated and 4 of them stated that they had taken and passed the CEH exam and another 3 said that they had scheduled the test (87%). The standard was met.

Interpretation of Results

Describe the extent to which this learning outcomes has been achieved by students *(Use both direct and indirect measure results)***:**
Two of the three factors were met. IT535 is given in the first year of the program and should cover the essential components of the certification exams. Later courses reinforce the concepts covered and confidence seemed to increase as the students progressed through the program.

Briefly describe program strengths and opportunities for improvement relative to assessment of outcome:

The overall program seems to work but students need to understand that they might need to cover the certification concepts more than once before they are in a position to take the higher-level exams. The faculty is currently mapping the main certification requirements (CEH, CSX, and CISSP) to the courses in the program to ensure that students understand the relationships.

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

AWS architecture certificate;
CSSIP bootcamp training
Changes in course content will be reviewed when the mapping is complete.

Learning Outcome 3: Optimize the effectiveness of cybersecurity in an organization by performing vulnerability assessments, risk mitigation, forensic analysis, auditing, certification and accreditation of information systems.

Assessment Activity

Outcome Measures *Explain how student learning will be measured and indicate whether it is direct or indirect.*	**Performance Standard** *Define and explain acceptable level of student performance.*	**Data Collection** *Discuss the data collected and student population*	**Analysis** *1) Describe the analysis process. 2) Present the findings of the analysis including the numbers participating and deemed acceptable.*
Direct: Performance on a forensic analysis in IT537, Computer Forensics and Incident response	70% of students were able to correctly find the solution to an assignment which required application of forensic techniques to a data corruption incident	The assignments were collected from Blackboard for the spring 2015 semester (12 students). The assignments were downloaded from Blackboard before they were graded by the professor	The assignment reports were evaluated by an adjunct who is a forensic specialist for the FBI and a full-time faculty member. 9 of the 12 students (75%) who submitted the assignment correctly analyzed the problem and identified the corrupted data. The standard was met.
Direct: Performance on an individual auditing project in IT 575 Information Security Management	70% of the students developed acceptable audit plans in an assignment in IT575, Information Security Management (3 or 4)	The assignments were collected from Blackboard for the fall 2014 semester (10 students). The assignments were downloaded from Blackboard by the professor as submitted by the students (no grades).	The assignment reports were evaluated by an adjunct who is an audit specialist for IBM, as well as by a fulltime faculty member. Emphasis was placed on the form, format, and writing of the audit plan 6 of the 10 students (60%) were scored as a 3 or 4. The major deficiency was considered the quality of the writing. The standard was not met.

Indirect: From the Graduating Student Survey, confidence that the student can use technology effectively in a workplace environment	80% of students should feel good or excellent about their ability to apply cybersecurity tools and techniques effectively.	Data was collected from the 2017-18 Graduating Student Survey, conducted by the Office of Institutional Effectiveness and looks at the response to the question: "Use technology effectively in a workplace environment."	19 students responded to the survey. One rated good and the second rated excellent to this question. It is not possible to draw and conclusions from this small sample.

Interpretation of Results

Extent this learning outcome has been achieved by students *(Use both direct and indirect measure results)***:**

Students appeared to have the desired cybersecurity knowledge, but communicating these results seems to be an issue.

Program strengths and opportunities for improvement relative to assessment of outcome:

The program covered the knowledge and skills required to work on complex problems in the cybersecurity area, however there needs to be more emphasis placed on oral and writing skills given the workplace need to communicate with people at many technical and management levels.

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

More writing assignments are being introduced in earlier courses and additional resource made available to students.

Appendices

Rubric 1: Evaluation of Cybersecurity Policy in IT570, Cybersecurity: Law, Policy and Compliance Requirements Engineering