MARYMOUNT UNIVERSITY
Arlington, Virginia

STUDENT LEARNING ASSESSMENT REPORT

PROGRAM: MS Cybersecurity
SUBMITTED BY: DIANE MURPHY DATE: NOVEMBER 16, 2016
BRIEFLY DESCRIBE WHERE AND HOW ARE DATA AND DOCUMENTS USED TO GENERATE THIS REPORT BEING STORED:
BLACKBOARD/CANVAS COURSES FOR 2015-16 FILING CABINETS IN BALLSTON 4040 ROOM 419

EXECUTIVE SUMMARY

Program description from the Course Catalog:

Marymount's cybersecurity Program is designed to prepare working professionals for high-level positions in cybersecurity 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, or industry.

Because of the university's proximity to federal agencies, including the Department of Homeland Security, the Department of Defense, and the 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.

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

This 36-credit program was originally offered primarily online. 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. Over the past year, classes have also been offered online and this has attracted a new set of students, including international students. The program is designed primarily for working professionals to prepare them for promotion to a cybersecurity leadership position, and to meet the certification requirements currently imposed on the profession, particularly by the Department of Defense on its employees and contractors. 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.

MARYMOUNT UNIVERSITY
Arlington, Virginia

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. Students may also take elective courses from the Forensic and Legal Psychology program, particularly those that focus on intelligence studies.

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

Learning Outcome	Assessment	Assessment	Year of Next Planned Assessment
1. Identify and solve cybersecurity issues in business and society by managing cybersecurity operations using available tools and techniques	2013-14 2014-15		2016-17
2. Review and understand the legal, regulatory, policy, and ethical issues related to securing cyberspace and ensuring the privacy of personally identifiable information (PII)	2013-14	**2015-16**	2018-19
3. Communicate effectively with others, including technologists and managers in the cybersecurity, IT, and users and managers in the business context	2013-14		2017-18
4. Use specialized knowledge and techniques to obtain skills and, if applicable, certifications in the cybersecurity field	2014-15		2016-17
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		2016-17
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**	2017-18
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**	2017-18

Describe how the program's outcomes support Marymount's mission, strategic plan, and relevant school plan:

The MS in Cybersecurity program is fully compliant with 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 (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). It recognizes the changing nature of the IT field and hence the need for life-long learning based on skills in information literacy and the ability to keep current with changes in the field.

In the 2011-12 school year, the President articulated a new "vision" for the university. The items in the vision statement that apply specifically to the graduate cybersecurity program include:

Academic Excellence

- Emphasize inquiry learning at all levels and provide students and faculty with opportunities for research collaboration.
- Offer programs that enable graduate students to develop the knowledge, skills, and values needed for professional success.
- Ensure a personalized education through small classes and faculty/student collaboration.
- Integrate an emphasis on ethics throughout the curriculum.
- Encourage cross-disciplinary collaboration.

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. Students are required to host a lab environment on their personal computers to carry out the labs and exercises at their work or home locations. These activities may occur through individual and group assignments. 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 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.

Community Engagement

- Use 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 that includes 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.

Student Profile

- Pursue opportunities for growth in key graduate programs.

The program has had a very successful start and we are currently exploring a DSc program in Cybersecurity. For the 2015-16 academic year, there were 40 students in Fall 2015, 32 in Spring 2016, and 29 in summer 2016 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 newer field of cybersecurity. A small number (4) were international students and a small number (3) are taking the dual MSIT/MS Cybersecurity program.

Provide a brief description of the assessment process used including strengths, challenges and planned improvements and provide evidence of the existence of a culture of continuous improvement based on assessment:

The program began in 2013 and the first 4 students graduated in December 2015. A further 7 students graduated in Spring and Summer 2016. The program has grown each year and 10 of the 11 graduating students are working in the field within two months of graduation. The last student is waiting for a security clearance to be processed before he can start work.

In 2015-16, 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 met individual adjunct faculty who were involved in providing data for the various assessment techniques. The results from the previous assessment were discussed, and this year's cybersecurity assessment plans discussed. 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 2014-15 outcomes assessment were discussed and data collection requirements 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 a specialties in health casre security, cyberintelligence, and data science.

MARYMOUNT UNIVERSITY
Arlington, Virginia

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.)*
Identify and solve cybersecurity issues in business and society by managing cybersecurity operations using available tools and techniques	We will continue to expose students to best practices in the cybersecurity field and to ensure students can apply their knowledge in the workplace.	The program has continued to evolve with more students and more adjunct faculty, professionals in the field who bring in real-world experiences. Two courses (IT530 and IT557) have increased their use of the day-to-day tools found in the cybersecurity operations environment. The emphasis is on students downloading the tools onto their own laptops so they can do assignments inside and outside the classroom.
Use specialized knowledge and techniques to obtain skills and, if applicable, certifications in the cybersecurity field	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. Changes in course content will be reviewed when the mapping is complete.	The mapping is still being finalized and will be issued shortly. In addition, we ran a non-cost 6-week boot camp for students to prepare for the Security+ certification in Spring 2016. 11 graduates and 3 undergraduate students attended and the evaluation were high.
Optimize the effectiveness of cybersecurity in an organization by performing vulnerability assessments, risk mitigation, forensic analysis, auditing, certification and accreditation of information systems	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	As seen in the attached mapping, we have increased the writing and oral presentation requirements in courses throughout the curriculum. We are also emphasizing students to use the Library Resources now

	communicate with people at many technical and management levels. More writing assignments are being introduced in earlier courses and additional resource made available to students.	given on the Canvas site for each course. At the end of each semester, we will survey students on their writing and presentation skills in selected courses and determine what extra support to offer next semester.

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

The committee found three outcomes as exemplary and 3 as adequate. The outcomes are being reviewed so that they are more generic and do not refer to a list of specific skills but use more generic terms (e.g., cyber defense techniques). An exit survey is under construction to get more detailed written feedback, currently the feedback is done in informal discussions.

MARYMOUNT UNIVERSITY
Arlington, Virginia

Outcomes Assessment 2015-2016

Learning Outcome 1: Review and understand the legal, regulatory, policy, and ethical issues related to securing cyberspace and ensuring the privacy of personally identifiable information (PII)

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** *Describe the analysis process. 2) Present the findings of the analysis including the numbers participating and deemed acceptable.*
Direct: In IT570: Cybersecurity: Laws, Policy, and Compliance, investigate the laws and regulations that cover an individual's privacy on the Internet.	80% of students were able to identify all laws and regulations that cover personal privacy in a specific industry in an assignment.	Assignments were downloaded from Blackboard before they were evaluated by the department chair based on a current list of laws and regulations provided by the professor.	The department chair measured the laws and regulations noted against a consolidated list of general and industry-specific laws and regulation, including those currently; under development and discussed in class. Students were expected to notify at least 100% of the most relevant laws and regulations as relevant to the scenario given 92.3% of the 26 students answered positively to these questions on the assignment and in spring 2016 100% of the 6 students responded correctly to all parts of the assignment. The outcome was met.
Indirect: Responses of gr4aduating students to two questions on their ability to perform ethically	80% of graduating students that answered good or excellent on two questions: "Determine the most ethically appropriate response to a situation" and "Understand the most ethical dilemmas in your field"	Data was collected from the 2015-16 Graduating Student Survey, conducted by the Office of Planning and Institutional Effectiveness	There were 7 responses to the survey. 100% of all the graduating students answered good or excellent The outcome was met.
Direct: Use of effective cybersecurity best practices to defend a system cyberattack	80% of students are able to successfully defend and document the scenario in	The assignments were collected from Blackboard for the spring 2016 semester	The responses were reviewed by a panel of three professors: The Chair, one full-time faculty member, and one adjunct faculty, all experts in the field of cybersecurity.

in the capstone course, IT670, Cybersecurity, Attack and Defend	IT670 and provide an adequate response (4 or more) on a scale of 0 (no response) to 5 (excellent), with respect to the legal and policy issues stated in the assignment	before they were graded by the professor.	Each panel member was given an opportunity to rate the solutions for their adherence to legal and policy in the field (0 through 5). These responses were averaged and 10 out of the 11 students (90.9%) received a 4.0 or more on average. The standard was met.

Interpretation of Results

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

All three outcomes in the areas of legal, policy, and ethics were met by MS in Cybersecurity students.

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

Cybersecurity attacks essentially break one or more Federal and local laws and we spend a great deal of time addressing the defense side: what is right and wrong in cyber defense as it pertains to law, policy, and ethics. Cybersecurity professional has access to the same tools as the cyber attacker and so it is important for them to understand the rights and wrongs of specific circumstances. Cybersecurity laws, regulations, and policy also vary by industry segment (government, healthcare, finance, etc.) and understanding these overarching documents is important for every cybersecurity professional. It is not just technical.

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

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 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.

MARYMOUNT UNIVERSITY
Arlington, Virginia

Learning Outcome 2: 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

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: Evaluation of communication activities in the cyber operations project of IT535, "Advanced Computer Security" which is a group project with a short deadline.	Students rate 70% of the team members as effective or very effective in the communication process on the cyber operations project in IT535, Advanced Computer Security, 8 out of 10 on the rubric (Rubric 1) is considered as effective	A questionnaire was given as a confidential evaluation by each student to evaluate their team as a whole and each member of the team was asked to assess the communication skills of each of the team members. There were xx students in Fall 2014 and xx students in Spring 2016.	There were xx students in the fall 2015 and a section with xx students in spring 2016. Of the xx total students, xx individuals rated their team or at least one of their team members as ineffective or only partially effective in their communications in teamwork leaving xx with a positive feeling about their team and its members (xx%). The most common complaint was the timeliness and quality of collaborative writing efforts. The standard was met.
Indirect: From the Graduating Student Survey, students showed confidence in their ability to work as part of a team and to lead a team	By the end of their program, 80% of students should feel good or adequate about their ability to cope in a team environment in the IT field where work is often fast-paced and deadline driven.	Data was collected from the 2014-15 Graduating Student Survey, conducted by the Office of Planning and Institutional Effectiveness. Responses to 2 questions were evaluated: 1) work as part of an effective team, 2) lead a team	100% of students felt confident in their ability to work as part of a team and 85.7% felt confident in their ability to lead a team. This standard was met.
Direct: Performance on a group project in an online course	Teammates rated 80% of their team members as effective or very effective communicators in working	A questionnaire was given to assess communication effectiveness as a confidential evaluation by one team	There were 16 students in IT585 in summer 2016. Of these 11 (68%) of student received 8 or more on the assigned rubric.

	on an online team project in IT585, Managing Technical People, in Summer 2016. 8 out of 10 is considered as effective on the rubric (Rubric 2).	member of another (2 or 3 person teams, selected by the instructor).	The standard was NOT met. Getting effective team work in asynchronous online classes remains a problem.

Interpretation of Results

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

Two of the three outcomes were met. The third team work in an online course remains an issue.

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

Group (team work) is emphasized in both face-to-face and online courses in the program**.** Group work in on-line courses has proved more difficult with students generally not being available for asynchronous sessions.

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

We are investigating online group techniques and when the research is complete we will distribute to the relevant faculty.

MARYMOUNT UNIVERSITY
Arlington, Virginia

Learning Outcome 3: 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

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: From the IT680, IT Masters Project, ability of students to perform an effective literature review in the cybersecurity field.	70% of students received a 2 or 3 on the rubric evaluation for the literature review (see rubric 3)	The literature review deliverable was reviewed by the program director and a librarian	73% of students received a 2 or 3 on the assessment. The standard for the outcome was met.
Indirect: From the Graduating Student Survey, confidence that the student can "find appropriate sources of information" and "evaluate the quality of information".	The performance standard is that 80% of students rated their ability to find appropriate sources and evaluate the quality of information as good or excellent.	Data was collected from the 20015-16 Graduating Student Survey, conducted by the Office of Institutional Effectiveness Data was reviewed for responses to two questions: "Find appropriate sources of information" "Evaluate the quality of information (e.g., scholarly articles, newspapers)"	85.7% of students rated themselves as good or excellent for both of these questions Passing this standard is important as information literacy is seen as important component for lifelong learning in the fast changing and growing field of cybersecurity. This outcome was met.
Indirect: From the Graduating Student Survey, confidence that the student can "apply knowledge and skills to new situations"	The performance standard is that 80% of students rated their ability to apply knowledge to new situations".	Data was collected from the 20015-16 Graduating Student Survey, conducted by the Office of Institutional Effectiveness	100% of students rated themselves as good or excellent in this category. Meeting this standard is also significant since IT is a fast changing field and new situations are always present.

MARYMOUNT UNIVERSITY
Arlington, Virginia

Interpretation of Results

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

All three outcomes were met.

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

Cybersecurity is a new and changing field and this is reinforced throughout the program. Most classes require students to discuss new items at the beginning of each class and reinforce the needs for the lifelong learning concept. The final master's project specifically addresses the concept of new knowledge and keeping current in the field.

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

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.