Marymount University

Academic Year : **2014-15** **Program:** **MS Cybersecurity**

STUDENT LEARNING ASSESSMENT REPORT
MS Cybersecurity

SUBMITTED BY: DIANE MURPHY **DATE: OCTOBER 25, 2015**
BRIEFLY DESCRIBE WHERE AND HOW ARE DATA AND DOCUMENTS USED TO GENERATE THIS REPORT BEING STORED:
BLACKBOARD COURSES FOR 2014-15 FILING CABINETS IN BALLSTON 4040 ROOM 419

EXECUTIVE SUMMARY

Marymount's Cybersecurity Program is designed to prepare working professionals 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, or industry.

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

This 36-credit program is 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. 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 is 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.

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.

List all of the program's learning outcomes

Learning Outcome	Year of Last	Year of Next Planned

	Assessment	Assessment
1. **Identify and solve cybersecurity issues in business and society by managing cybersecurity operations using available tools and techniques**	2013-14	**2014-15**
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
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**
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**
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
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

Marymount's MS in Cybersecurity Program is designed to prepare working professionals 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, government contractors, cybersecurity product vendors, nonprofits, and industry.

The program began in 2013 and the first 4 students graduated in December 2014.

Because of the university's proximity to federal agencies, including the Department of Homeland Security, the Department of Defense, the National Security Agency, and the National Science Foundation, faculty members 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 adjuncts and guest speakers at the many Cyber Center events, designed to supplement the online courses.

This 36-credit program is 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. 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 can 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.

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 my occur through individual and group assignments. Cybersecurity graduate classes have averaged around 14 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.

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 2014-15 academic year, there were 31 students in Fall semester and 28 in Spring 2014. 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 (2) 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:

In 2014-15, the assessment process was successful and cybersecurity faculty responded well to all calls for data (full-time and part-time). There was some confusion about the data from the fall 2014 semester as this was misplaced by a graduate assistant during the move. The documents were misfiled but were later found.

Outcome assessment techniques were discussed early at a department meeting of cybersecurity faculty. The results from the previous assessment were discussed, and the cybersecurity plans discussed. A plan was put in place to focus on both teamwork and ethical decision making in the designated courses. Outcomes and their measurement for the 2014-15 outcomes assessment were discussed and data collection requirements identified.

A number of other initiatives were also identified as part of our continuous improvement process including the need for an "internship" program. In addition, there is an increasing demand for face-to-face in addition to on-line offerings and the scheduling implications are being studied.

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	The courses seemed to be successful in developing students who have the knowledge and skills to understand the cybersecurity field and to be able to develop a policy that implements that cybersecurity posture. No changes in the two courses (IT530 and IT570) were anticipated until more students have taken the courses.	We reviewed IT570 in Fall 2014 and revamped it in Spring 2015 to allow for more in class discussions and to focus more on the latest developments in the field. New course materials were identified.
Review and understand the legal, regulatory, policy, and ethical issues related to securing cyberspace and ensuring the privacy of personally identifiable information (PII)	The program seems to satisfactorily cover the privacy and ethics requirements of the learning outcomes. There were no changes planned this early in the program	Two faculty members (Donna Schaeffer and Michelle Liu) researched cybersecurity ethics in detail as part of a potential NSF grant submission. Some of these results will be added to IT530 in Fall 2015 and IT570 in Spring 2016.
Communicate effectively with others, including technologists and managers in the cybersecurity, IT, and users and managers in the business context	Communication online is difficult. The discussion board seemed to work but not other group activities or written assignments. The faculty will address how to introduce writing techniques into the graduate program more effectively.	The cybersecurity faculty discussed writing across the curriculum at a special meeting held in November 2014 and 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 attend one of the writing seminars given By Patrice Scanlon in the SBA.

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

This was the first year of the program and the assessment committee rightfully noted that the outcome results were very generic and also noted that there were no indirect measures. At that time, there were no graduates from the program and so no Graduating Student Survey data. As required by the committee, a detailed assessment plan was produced for the 2014-15 year and submitted to the Office of Planning and Institutional Effectiveness (PIE) based on the input from a special meeting of the cybersecurity faculty in November 2014 and consultation with PIE. The catalog copy was modified to reflect the learning outcomes developed during the assessment process. (see 2015-16 catalog).

Outcome and Past Assessment

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

Is this outcome being reexamined? Yes

In 2013-14, the courses were considered to be successful but it was recognized that only a small number of students were enrolled in the program. The numbers have grown each semester with 28 students in the program in Spring 2014.

Assessment Activity

Outcome Measures	Performance Standard	Data Collection	Analysis.
Direct: Use of effective cybersecurity best practices to defend a system cyberattack in the capstone course, IT670, Cybersecurity, Attack and Defend	70% of students are able to successfully defend and effectively document findings for an attack scenario 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 Blackboard for the fall 2014 (12 students) semester and spring 2015 semester (11 students). The assignments were downloaded from Blackboard before they were graded by the professor.	The responses were reviewed by a panel of three professors: the Chair, 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). 18 of the 22 students (82%) obtained an average of 4 or more on the rubric. 1 student did not submit a response to the assignment. The standard was met.
Direct: Development of an effective policy document as part of Assignment 3 in IT570, Cybersecurity: Law, Policy and Compliance.	70% of all students generate an effective policy in response to a class assignment which focuses on managing cybersecurity operations (a grade of 18 or more on the rubric)	The assignments were collected from Blackboard for the fall 2014 semester The assignments for 13 students were downloaded before they were graded by the professor.	The responses were reviewed by an adjunct from the Federal government and a full-time faculty member, both experts in cybersecurity, and rated according to a rubric (see Rubric 1). 10 of the 13 students achieved 18 or more on the rubric (77%), with 3 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 2014-15 Graduating Student Survey, conducted by the Office of Institutional Effectiveness	Only 2 students responded t0 the survey. One rated it 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

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

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.

Outcome and Past Assessment

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

Is this outcome being reexamined? No

Assessment Activity

Outcome Measures	Performance Standard	Data Collection	Analysis
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 and4 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

Extent this Learning Outcome has been achieved by students

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.

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

Changes in course content will be reviewed when the mapping is complete.

Outcome and Past Assessment

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.

Is this outcome being reexamined? No

Assessment Activity

Outcome Measures	Performance Standard	Data Collection	Analysis
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 full-time 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	80% of students should feel good or excellent about their ability to apply cybersecurity tools and techniques effectively.	Data was collected from the 20014-15 Graduating Student Survey, conducted by the Office of Institutional Effectiveness and looks at the	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.

workplace environment		response to the question: “Use technology effectively in a workplace environment.”	

Interpretation of Results

Extent this Learning Outcome has been achieved by students:

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.

Attachments
Rubric 1: 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	