Designing a Masters Program in Cybersecurity and Leadership

Bryan S. Goda Robert Friedman
godab@uw.edu rsfit@u.washington.edu

University of Washington, Tacoma
Institute of Technology
Tacoma, Washington, USA 98405

ABSTRACT

The Master of Cybersecurity and Leadership (MCL) taught at the University of Washington Tacoma is a partnership between the Institute of Technology and the Milgard School of Business. The 10-course graduate level program was initially benchmarked against existing masters programs, surveys of prospective student population were conducted, and an assessment was done on the estimated demand for MCL graduates in the region. The program outcomes were then mapped against the course objectives to insure the correct mix of courses and topics. The program's admission requirements and schedule were then tailored to our expected pool of applicants. The MCL program is proposed to start in January 2013.

This paper discusses the design process and possible ways to reduce risk in the start-up of a new degree program. How a program is marketed to prospective students and what program graduates will do after program completion is just as important as the initial design of the program. Planning for the administration of the program and the assessment process is an important phase of the initial design.

Categories and Subject Descriptors

K.3.2 [Computers and Education]: Computer and Information Science Education – Information Technology Education.

General Terms

Degree Programs, Design

Keywords

Information Technology Education, Cybersecurity

1. INTRODUCTION

The University of Washington Tacoma (UWT) was founded in 1990 to meet regional needs for community college transfer students. UWT is set in downtown Tacoma's Union Station neighborhood, a district of historic warehouses. The vision of the University is to provide access to an exceptional university education; provide an interdisciplinary approach to knowledge and discovery in the 21st century; and develop a strong and mutually supportive relationship between the campus and its surrounding communities. The MCL program leverages the resources of the University of Washington's Center for Information Assurance and Cyber Security by extending the reach of the Center's related certification courses to new military populations in the South Sound region of Washington State. By identifying, addressing, and promoting solutions for issues of information assurance and cyber security, MCL will serve as an educational foundation for invention, innovation, and entrepreneurship in the state of Washington, thereby sustaining the vitality of existing and prospective information assurance and cyber security industries.

SIGITE'12, October 11–13, 2012, Calgary, Alberta, Canada.
Copyright 2012 ACM 978-1-4503-1464-0/12/10...$15.00.

2. PROGRAM DEVELOPMENT

A benchmarking of similar programs concludes that there are no similar programs in Washington State and most of the similar programs are located on the east coast of the US. The University of Maryland, Virginia College, Washington Governor's University, Utica College, and New York University offer online master degrees in cyber security [1,2,3,4,5], while George Washington University, New Jersey Institute of Technology, and American University offer it as part of their resident computer science degree [6,7,8]. The National Defense University offers a Government Information Leadership [9] master's degree, the program most similar to the MCL program.

The Joint Base Lewis McChord (JBLM) and the Naval Bases at Bremerton and Bangor near UWT have a pool of 3000 junior officers who would be attracted to an MCL type program. Many of these officers work in units that specialize in Information Assurance or need better organizational leadership skills. While a masters degree is not required for promotion, a masters degree in cybersecurity and leadership would enhance unit performance. An interest survey was conducted at a National Guard unit specializing in information warfare and the local commanders were interviewed. The feedback was overwhelming support for the startup of a new program. Auburn University has created a master in cybersecurity with a similar officer population at Maxwell Air Force Base [10]. The Institute of Technology at UWT offers BS degrees in Computer Science, Computer Engineering, Information Technology and a graduate program in Computer Science. Students majoring in Information Technology have also shown a keen interest in the MCL program.

The Information Technology field is expected to be one of the top two employment growth areas, with an expected increase in demand of 23% [11]. The I-5 corridor around UWT is home to such tech savvy companies as Microsoft, Amazon, Boeing, Liberty Mutual, Pacific Medical Centers, KPMG, and the Port of Tacoma. Companies are looking for programs that can produce managers and technology leaders who can design, implement, and manage cybersecurity systems. Complex distributed systems operating in a mobile, cloud computing environment demand skilled professionals highly trained in cybersecurity.

On April 27, 2009, in a speech to the National Academy of Sciences, President Obama called for major investments in attracting students to science and engineering, because science is now "more essential for our prosperity, our security, our health, our environment, and our quality of life than it has ever been before." James Gosler, a veteran cyber security specialist who has worked at the CIA, the National Security Agency and the Energy Department, says we do not have enough talented cyber workers coming into the field to support national security objectives. James Gosler and System Administration, Networking and Security Institute (SANS) Research Director Alan Paller estimate that there are only 1,000 highly skilled cyber defense specialists in the U.S., but that the nation needs 20,000 to 30,000 of these skilled workers to meet national computer security needs [12].

3. Program Design

The MCL program will combine coursework in both the cyber security (technical) and leadership (organizational/strategic) areas. It is designed to have students from a wide variety of technical backgrounds. Since UW is certified by the National Security Agency as a Center of Excellence in Information Assurance, this program will help in the continued certification of the university. The MCL will expose students to a Common Body of Knowledge in preparation for the Certified Information Systems Security Professional (CISSP) examination. Upon completion of the program, students should be able meet the program outcomes specified in Table 1.

1. Be able to identify and critically assess issues and concepts related to the protection of information and information systems. Develop and articulate an organization's strategic direction.
2. Assess an organization's security attributes: confidentiality, integrity, and availability. Understand an organization as complex, interdependent system operating in an ever-changing and uncertain environment.
3. Analyze and evaluate proposed or extant information security policies, practices, and procedures in order to assess potential advantages and disadvantages that might flow from implementing them. Provide leadership so that confidentiality, integrity and availability can be protected. Insure an environment of threat reduction is maintained in an organization.
4. Use risk management principles to assess threats, vulnerabilities, countermeasures and impact contributions to risk in information systems. Perform a risk analysis for an environment. Create a management plan for security in an environment. Analyze and diagnose complex organizational problems, design effective solutions, and implement change.
5. Create policies, strategies and standard operating procedures for securing information and communication systems. Manage people, information, and processes to accomplish organizational goals and objectives.
6. Identify and critically assess the social political, economic, and ethical dimensions of IA and CS in an organizational context.

Table 1. Program Outcomes for the MCL

The MCL program was designed to accommodate students in the military who are normally working during the day. MCL will consist of ten 4-credit courses of eight week durations. The program is a joint venture of the Institute of Technology and the Milgard School of Business. The Institute of Technology will teach 5 cybersecurity courses and the Milgard School of Business will teach 5 courses from their Masters of Business Administration program. Courses will run 4 hours one night per week, which allows a cohort to complete the program in a calendar year.

Module 1
Principles of Cyber Security
Business Communication

Module 2
Information Assurance / Cybersecurity and Risk Management in Context
Business Ethics and Social Responsibility

Module 3
Designing and Executing Information Assurance and Cybersecurity Strategies
Strategic Management

Module 4
Network and Internet Security
Individual and Group Dynamics

Module 5
Building an Information Risk Management Toolkit
Organization Change

The modules are designed to build on a student's prior experience in a previous module. Prior to entering Module 1, most students should have experience working in an organizational environment and have taken the recommended background coursework in information technology. In Module 1, students will be exposed to the concepts, strategies and skills related to the life cycle of information assurance. The Principles of Cybersecurity will cover information assurance organizational goals, the threat spectrum, risk, and legal/ethical issues. The Business Communication course promotes the understanding of important communication dynamics and the ability to communicate strategically and professionally in organizations.

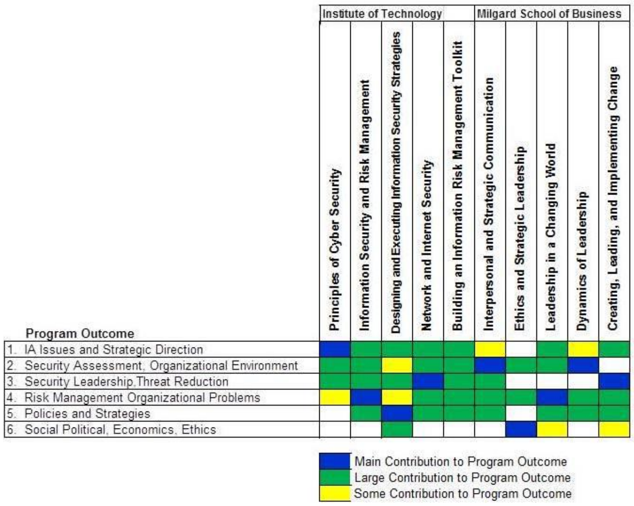
Module 2 builds on the introductory material presented in Module 1 and examines risk management involving assessment, analysis and mitigation planning. Students will be able to evaluate polices, practices, and procedures to determine overall advantages and disadvantages from implementation. The Business Ethics course will focus on the ethical and moral challenges facing business managers today. The combination of both of these courses is that our graduates will be able to evaluate alternatives and determine if they conform to ethical standards.

Module 3's courses on designing cybersecurity strategies and strategic management will focus on how to effectively direct an organization's direction. Students will be working on case studies that allow students to apply what they have learned in Modules 1 and 2. Students will be halfway through the program and should be able to appreciate how the cybersecurity and leadership courses complement each other.

Module 4 provides the skills necessary for securing networks, email, and cryptographic methods. The Individual and Group Dynamics course prepares our graduates to assemble the skills, talents, and resources of individuals and groups to solve problems. So we have an electronic network as well as a human network being implemented during the Module 4.

Module 5 is designed to tie the previous 8 courses together so that our graduates will have the necessary tools to develop security architectures. The Organizational Change course will have students apply these concepts to real organizations and assess their own managerial skill as they relate to creating and reacting to change.

Each of the course objectives was mapped to the program outcomes to insure a balanced coverage of topics. Figure 1 shows that balance among the courses.



	Institute of Technology					Milgard School of Business				
Program Outcome	Principles of Cyber Security	Information Security and Risk Management	Designing and Executing Information Security Strategies	Network and Internet Security	Building an Information Risk Management Toolkit	Interpersonal and Strategic Communication	Ethics and Strategic Leadership	Leadership in a Changing World	Dynamics of Leadership	Creating, Leading, and Implementing Change
1. IA Issues and Strategic Direction	🟦	🟩	🟩	🟩	🟩	🟨		🟩	🟨	🟩
2. Security Assessment, Organizational Environment	🟩	🟩	🟨	🟩	🟩	🟦	🟩	🟩	🟦	
3. Security Leadership,Threat Reduction	🟩	🟩	🟩	🟦	🟩	🟩				🟦
4. Risk Management Organizational Problems	🟨	🟦	🟨	🟩	🟩	🟩	🟩	🟦	🟩	🟩
5. Policies and Strategies		🟩	🟦	🟩	🟩	🟩		🟩	🟩	🟩
6. Social Political, Economics, Ethics			🟩				🟦	🟨		🟨

🟦 Main Contribution to Program Outcome
🟩 Large Contribution to Program Outcome
🟨 Some Contribution to Program Outcome

Figure 1. Program Outcomes Mapped to Courses.

The student population entering into the MCL program will likely have a wide variety of skills and backgrounds, some not necessarily in a science and technology area. It was determined the admission requirements should be based on the graduate programs of the Milgard School of Business and other cybersecurity graduate programs, and that each entrant should have a grounding in information technology. Admission requirements to the program are:

- Bachelor’s Degree from a US Institution or equivalent
- Minimum Grade Point Average of 3.0 on a 4.0 scale
- Competitive scores from the Graduate Record Exam
- Fluency with Information Technology

The potential student pool of applicants will come from the National Guard, alumni of Bachelors of Information Technology and Systems program, and from the enlisted ranks of Joint Base Lewis/McChord. Working professionals in the public, private, and non-profit sectors will be interested in expanding career choices in Information Assurance and Cybersecurity. These individuals desire to learn more about advanced cyber- security concepts, strategies and methods in order to improve their performance in their current job, progress faster in their careers, or transition to a new career field. Table 2 depicts the projected growth of the MCL program.

Year	1 2013	2 2014	3 2015	4 2016	5 2017
Students	24	30	40	50	50
Graduates	21	27	36	45	45

Table 2. Projected Growth of MCL Program

The quality of the curriculum and the UWT faculty will create a positive reputation for the MCL program, resulting in organic growth over the life of the program. Additionally, despite recent budget constraints and tuition increases, UWT’s enrollments continue to increase. This fee-based program will be charging tuition that can be accommodated by the 9-11 GI Bill benefits. This is a relatively unexplored source of enrollment, but the number of potential students and the enthusiasm expressed by JBLM and National Guard Camp Murray officers suggests that there could be significantly positive potential in student enrollments and the revenue base. There is a certain advantage in being a first mover in this direction. Though the proposed MCL program is designed initially for military personnel, it could potentially also attract career-changing college graduates, as indicated by interest from the Healthcare Leadership program at UWT.

The admission process of the MCL program will make effective use of the UWT diversity policy. It will also maintain and enhance the School’s existing diversity perspective in its undergraduate and graduate admission processes. Program advertising materials will be used in regional and local newspaper/magazine and academic/education websites. Working with the UWT’s Assistant Chancellor for Equity and Diversity, a number of media outlets will help to provide outreach to underrepresented minorities. While maintaining consistency of admission criteria in screening student applications, diversity among the admitted students will ensure a robust and exciting learning environment.

4. Administration and Assessment

The MCL will require incremental resources in the administration of the program and student advising. This includes (1) co-program directors to oversee the academic program; and (2) one half-time staff person, whose responsibilities will be related to admissions, tracking, maintaining program guidelines, course scheduling, coordinating with the administration and student services staff, students counseling, verifying student requirement fulfillment for graduation and similar tasks. The admission process will be handled by a faculty committee, similar to those in our current MBA and MS-CSS programs. The program directors will be selected from the management faculty of the Milgard School and the ITS faculty in the Institute, and may be compensated in the form of course release or stipend for the additional administrative responsibilities assumed, if necessary. The staffing of the program will be fully supported by the revenue generated by the MCL program and will not require any state funding.

MCL will have an annual online course and program evaluation survey to assess the program. There will also be group discussions to get feedback on the courses and program. Student course evaluations and classroom assessments (peer evaluations) will also be an integral part of the assessment process. Faculty will consider this information and recommend improvements to the program. Faculty teaching MCL courses with an embedded measure of key learning objectives will also discuss results from the prior year, their plans for modifying course assignments based on data and any changes to evaluation criteria used. Additionally, the faculty will discuss what they cover in their MCL courses and how they can better integrate their efforts.

The program leadership will hold focus groups with managers at organizations that employ MCL graduates to garner feedback towards continuous improvement of the program. Similarly, there will be follow-up focus groups with MCL alumni to gather feedback based on their work experience and how well the program prepared them for careers in cybersecurity.

5. CONCLUSIONS

The lack of a graduate program in cybersecurity in a technology heavy region fills a need that students, employers, and the community desires. Careful research is required prior to launching a new program, else it is doomed to fail. A graduate program needs to be designed from the top-down, so that the courses support the program outcomes. The administration and assessment of the program have to be considered early-on in the design process, because a new program will evolve and grow as it becomes mature. Cybersecurity is a new area that encompasses several disciplines. Merging leadership skills with technological expertise is an exciting combination with a bright outlook.

This paper proposes a new advancement in the field of Computer Science education by combining the fields of cybersecurity and leadership together into a graduate degree. The idea of a modular design where students will steadily progress into becoming cybersecurity professionals with an acute business sense makes them very attractive to future employers and can further promote cooperation between business schools and technology programs.

REFERENCES

[1] University of Maryland. Retrieved May 16, 2012 from http://cyber.umd.edu/education/index.html

[2] Virginia College Online Programs. Retrieved May 16, 2012 from http://www.vconline.edu/graduate-degrees-online/cyber-security-degree.cfm

[3] Washington Governor's University. Retrieved May 16 2012 from http://washington.wgu.edu/online_it_degrees/information_security_assurance_degree

[4] Utica College Cyber Security – Intelligence and Forensics. Retrieved May 16, 2012 from http://www.onlineuticacollege.com/programs/masters-cybersecurity.asp

[5] NYU-ePoly Cybersecruity MS. Retrieved May 16, 2012 from http://cs.njit.edu/academics/graduate/mscsp.php

[6] Department of Computer Science, George Washington University. Retrieved May 16, 2012 from http://www.cs.gwu.edu/academics/graduate_programs/master/cybersecurity/program-requirements

[7] Master of Science in Cyber Security and Privacy NJIT. Retrieved May 16, 2012 from http://cs.njit.edu/academics/graduate/mscsp.php

[8] Master of Arts in Intelligence Studies, American Military University. Retrieved May 16, 2012 from http://cs.njit.edu/academics/graduate/mscsp.php

[9] National Defense University Cyber Security Program. Retrieved May 16, 2012 from http://cs.njit.edu/academics/graduate/mscsp.php

[10] Top Career Fields. Retrieved May 16, 2012 from http://www.moneycrashers.com/5-great-career-fields-for-the-future/

[11] Sahinoglu, M., Cybersystems and Information Security Master of Science Program at Auburn University Montgomery. *GSFT International Journal on Computing, Vol 1, No.3,* August 2011. 70-76.

[12] Gjelten, T., Cyber Warrior Shortage Threatens U.S. Security. Retrieved October 6, 2010 from National Public Radio: http://www.npr.org/templates/story/story.php?storyId=128574055s

[13] Petrova, K., Kaskenpalo, P., Philpott, A., Buchan, J., Enbedding Information Security Curricula in Existing Programmes. In *InforSecCD Conference '04,* pages 20-29, Kennesaw GA, USA, 2005. ACM Press.

[14] Bacon, T., Tikekar, R., Experiences With Developing A Computer Security Information Assurance Curriculum, In *Consortium for Computing in Small Colleges*, 2003, 254-267.

[15] Taylor, C., Ednicott-Popovsky, B., Phillips, A., Forensics Education: Assessment and Measures of Excellence. In *Proceedings of the 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering*, Seattle WA, USA, April 10-12, 2007. IEEE Computer Society.

[16] Polson, C., Persyn, J., Cupp, O., Partnership In Progress: A Model for Development of a Homeland Security Graduate Degree Program. *Homeland Security Affairs*, Vol VI., No. 2, May 2010.