**Abstract**

The Master of Cybersecurity and Leadership (MCL) is a partnership between the Institute of Technology and the Business School. The University’s mission is to serve the education needs of the community. Cybersecurity is a promising area because business, military, government, and utilities all desire trained cybersecurity professionals that can lead and effect change. This paper discusses the design process and possible ways to reduce risk in the start-up of a new degree program. Careful market assessment regarding potential students as well as employers who are willing to hire graduates are important initial first steps that also inform a program’s design. Planning for the administration of the program and how the curriculum gives students the critical competencies needed to succeed in the workplace are also important. We highlight several ways the curriculum links students to employers including but not limited to an innovative Cybersecurity Challenge, a partnership with local government and businesses that provides students practical opportunities to demonstrate their cybersecurity leadership/technical knowledge.

**History and Overview of the MCL Program**

 Our University was founded in 1990 to meet regional needs for community college transfer students. The goals of the University are to provide access to an exceptional university education, to offer an interdisciplinary approach to knowledge and discovery in the 21st century, and to develop a strong and mutually supportive relationship between the campus and its surrounding communities. The campus has revitalized the downtown area, a district of historic warehouses, and the campus has grown steadily since inception.

 Launched in 1994, the Business School offers an undergraduate degree in business administration, three graduate programs, and serves over 660 students. Founded in 2001 with an initial cohort of 30 Computer Science students, the Institute of Technology is on its way to becoming a polytechnic that supports multiple degree programs providing an educated technical work force for the state. Today, in 2014, the Institute has three undergraduate and two graduate degree programs with 640 students currently enrolled.

 Approached by the National Guard who wanted to have a professional cybersecurity degree program that would support their mission to respond to cybersecurity attacks on our nation’s infrastructure, leaders from the Institute of Technology and the Business School began to explore a joint degree program in 2012 (Goda & Friedman, 2012). These leaders envisioned a curriculum that would combine a technological education in cybersecurity design with managerial and leadership skills. They believed that graduates of such a program would be well positioned to lead and manage teams within an organization’s information technology function and to advocate for the role that cybersecurity plays in furthering an organization’s performance and effectiveness.

The startup of any new Masters program can be a risky proposition. Basic questions need to be answered including, “What is the demand for this program? What skills should graduates have? Will there be jobs for them and who will hire them after they leave the program?” The process by which the MCL program was initially assessed and ultimately designed helped to answer these questions and mitigate the risk associated with a mounting a new program.

One factor that reduced risk was the ever growing demand for cybersecurity personnel. In 2012, early evidence suggested healthy demand for graduates capable of designing, implementing, and managing cybersecurity systems. For example, 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” (Obama, 2009). James Gosler, a veteran cyber security specialist who has worked at the CIA, the National Security Agency and the Energy Department, claims we do not have enough talented cyber workers coming into the field to support national security objectives (Gjelten, 2010). 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 (Gjelten, 2010). National demand for cybersecurity professionals continues to increase and shows no signs of diminishing (CSFI, 2014). Moreover, more recent research suggests that senior cyber leaders who can effectively communicate cyber related business cases and return on investment, relying on persuasion and negotiation in a complex business environment are in even shorter supply (CSFI, 2014).

 Local demand and supply conditions also appeared favorable for a program in cybersecurity leadership. The area is home to such tech savvy companies as Microsoft, Amazon, Boeing, Liberty Mutual, Pacific Medical Centers, KPMG, and the Port, all of whom are likely to need cybersecurity leaders. In addition, on the supply side, the winding down of military engagements across the world means a potential steady stream of military personnel looking to transition to the private sector. The University’s proximity to the Army and Air Force bases and the Air and Army National Guard provide a plethora of active duty, National Guard and Reserve personnel. Moreover, the bases are surrounded by a veteran rich population (1 out of every 11 citizens in the state is a veteran). Early on the thinking was that the MCL’s dual focus on technology and management would be particularly attractive to military and technology personnel wishing to transition into higher-level corporate and government leadership positions.

 In order to further explore the potential local demand for an MCL degree program, initial ideas were circulated among constituents such as the Institute Advisory Board, local industries, and government agencies, all of whom expressed great enthusiasm. In addition, the leaders conducted an informal benchmarking exercise to ascertain the degree of local and national competition, if any. At the time, the exercise revealed that no similar programs existed in the state and that most other similar programs were located on the East coast of the U.S. A number of schools offer online master degrees in cyber security or as part of their resident computer science degree. See Table 1 for examples. In particular, the exercise found only one program that was at all similar to the MCL, namely the National Defense University’s Government Information Leadership Master’s degree. This program provides graduate-level information security instruction for those serving as Chief Information Security Officers in government organizations. In general, the search for other graduate degree programs in cybersecurity revealed few programs that combine business leadership courses with cybersecurity courses, especially on the West coast[[1]](#footnote-1).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| School | Degree Title | Credits Hours | Year Established | Online or Resident |
| Our Program | MCL | 40 | 2013 | Resident |
| George Washington University | MS in Cybersecurity | 30 | 2013 | Resident |
| Univ of Maryland | ME in Cybersecurity | 30 | 2011 | Both |
| National Defense University | Government Information Leader | 39 | 2010 | Resident |
| New Jersey Institute of Technology | MS in Cybersecurity and Privacy | 30 | 2011 | Resident |
| Utica College | MS in Cybersecurity | 30 | 2010 | Online |
| Virginia College | MS in Cybersecurity | 56 | 2010 | Online |
| Washington Governor’s Univ | MS in Information Security and Assurance | 30 | 2010 | Online |

Table 1. Comparison of Cybersecurity Masters Degrees[[2]](#footnote-2)

 These efforts to understand the potential for an ample supply of potential students in the local area, ascertain the degree of interest in employing graduates from regional employers, and the search for existing competitors helped mitigate the risk of starting a new program. Indeed, the attractive supply and demand conditions coupled with strong support from campus administration convinced the leadership to pursue developing the MCL program. But risk isn’t reduced solely in the processes that lead up to the choice to pursue a new program; risk can also be mitigated through the ways a program is designed and implemented. Below, we highlight the main features of the MCL program and how some of these also serve to reduce risk.

**Design of the Program**

 The MCL curriculum combines coursework in both the cybersecurity (technical) and leadership (management/organizational/strategic) areas. It is a traditional program with resident instruction and is structured on a cohort basis where students take a locked sequence of courses together. The program is ideally suited for students with both a technical background in network design and some degree of work experience. The goal of the program is to produce students who will both understand the basic technological issues surrounding cybersecurity and be able to manage people, information and processes to accomplish broader organizational and business goals.

 On the technical side, the MCL program exposes students to Common Body of Knowledge and the topics covered on the Certified Information Systems Security Professional (CISSP) examination. And on the managerial side, the MCL program gives students the perspective and understanding of an organizational leader that extends beyond the IT function. Upon completion of the program, students should be able meet the program outcomes specified in Table 2.

|  |
| --- |
| 1. Identify and critically assess issues and concepts related to the protection of information and information systems.
2. Use risk management principles to assess threats, vulnerabilities, countermeasures and impact contributions at risk in information systems.
3. Create policies and standard operating procedures for organizations that are ethically, morally and legally sound.
4. Illustrate and explain fundamental architectures of networks and the Internet, as well as their underlying protocols.
5. Understand the concepts inherent in information security architectures.
6. Understand the key functions and challenges of organizational communication, including the factors that can hinder and facilitate effective communication in business settings.
7. Recognize ethical dilemmas and social responsibilities.
8. Formulate and implement strategy and effectively manage change.
 |

Table 2. Program Outcomes for the MCL

 Although it is a full time program, the MCL program accommodates students who are normally working during the day. This expands the potential pool of students to those who are already employed and also require full time enrollment status. Students attend classes two nights a week, with only small parts of some courses being offered online. In its first year of operation, the program received 45 applications and offered admissions to 32. 30 accepted and 27 are in the final stages of completion, which is well over the projected class size of 20. Approximately 60% of the first year cohort students are military related including Active Duty, Reserves, National Guard, veterans and retirees.

The program consists of eight 5-credit courses which are designed and taught by faculty from the Institute of Technology and the Business School. Two classes are offered each quarter for a total of 40 credits:

 Autumn Quarter (Introduction)

*Principles of Cybersecurity* provides an overview of the ten domains of
 cybersecurity.

 *Principles of Business* provides an overview of key concepts in business including
business communication, marketing, ethics, accounting and financial analysis.

Winter Quarter

*Information Assurance, Risk Management, and Security Strategies* exposes
students to key risk assessment and management frameworks, which enables
them to assess and prioritize risk in an organizational setting and communicate
these risks to high level decision makers.

 *Individual and Group Dynamics* prepares students to establish, manage and lead
high-performing, successful teams and to lead their own careers effectively.

Spring Quarter

*Network and Internet Security* insures that students are exposed to the current
industry best practices, such as white listing, intrusion detection systems, and
the other technical and policy concepts covered under the CISSP preparation, as
well as the focus of government organizations, such as defense in depth,
constant monitoring, and incident response preparedness.

 *Strategic Organizational Change* explores the repertoire of concepts, tools, and
techniques for understanding the strategic management of organizations and
how successful leaders and change agents can create, implement, and manage
change.

Summer Quarter (Capstone)
 *Cybersecurity Management* provides a framework to support the Cybersecurity
 Challenge with consultants and periodic updates.

*Project Management* explores project challenges from a business administration
point of view.

Figure 1 links the main topics of each of these courses and the level of their contribution to the program outcomes. All of the courses focus on preparing the student to work on a team solving a capstone cybersecurity project.



Figure 1. Mapping of Program Outcomes to Courses

 A full-time advisor was hired to support the program and to more fully serve the local pool of potential students coming from a military background. While there are active duty officers and senior enlisted seeking a master’s degree for promotional purposes, many service members are preparing for retirement or forced transition to civilian careers as a result of the drawn down cycle.  Thus, the presence of a dedicated advisor who understands these dynamics is critical to the program’s success. Encouraging  these mid-career professionals through the application process, guiding them through the Graduate Record Exam (GRE) and supporting them as they face a transition from military to academic culture builds rapport, trust and goodwill in the community. During the application process, the advisor identifies immediate and long term career goals, and during the program students receive individualized coaching sessions and workshops enabling them to achieve their goals. Such individual attention increases enrollment as well as retention, two key factors in determining the success of a program.

 Additional administrative aspects that mitigate risk and increase the chances of a vibrant and healthy pipeline of satisfied students include advertising efforts as well as carefully planning for monitoring the program over time. Advertising helps to attract students to the program. Due to its newness and innovative design, the MCL program has been featured on National Public Radio, local radio, magazines, and newspapers which helps draw in students. In addition, planning for ongoing assessment enables faculty and administration to be responsive to student needs, especially in the early days. Students are given a survey at the end of every course to assess how to improve each course. Periodic discussion groups are used to gauge student morale and to assess what they are getting out of the classes thus far. Our ultimate measure of success is how our students do in the workplace, either in their current company or in a new company. At the time of the writing of this article, the first cohort is a little more than halfway through the program, and already, four students have found excellent cybersecurity positions out of the seven students seeking employment.

**Innovations in Curricular Design and Administration**

 In addition to the courses students take, the presence of a dedicated advisor, and the other administrative elements that contribute to the program’s success, additional innovations in curricular design create a rich and meaningful experience for students in the program. Below we summarize the major activities and the kinds of experiences we have created for students in the MCL program.

 **Optional Support for CISSP.** The Principles of Cybersecurity course is an introductory course designed to give the student an overview of cybersecurity and for some, it provides additional support to sit for the CISSP exam. The reference book for this type of course is Shon Harris’ Certified Information Systems Security Professional Exam Guide (Harris, 2012) because it covers all ten domains of cybersecurity and comes with online quizzes and videos. This book is used by the students throughout the program and serves as a roadmap for the areas they can specialize in. About 1/3 of the students attended an optional, free CISSP boot camp offered to all students. The optional boot camp allowed those students with the requisite experience who were intending to use the GI bill to pay for the CISSP exam to prepare for the exam. Even though the current employment market is flooded with more and more certifications in every area of specialization, the CISSP is a universally recognized milestone (ISC 2014) that helps to set these graduate apart from other applicants. Approximately 50% of the first cohort of students have the requisite experience in two of the ten domains required for the CISSP. It is not a goal of the program to have every student pass the CISSP, rather the program encourages it to be a long range goal for students to achieve. Students are informed about the CISSP associate level, where they can take the exam now and earn the required experience later. Three of the initial cohort entered with CISSP credentials and an additional five students have taken the CISSP while in the program and passed.

 **Real-World Information Assurance Strategies.** A major theme of the program is the development of student expertise in the area of information security and risk management. Students examine real world cases studies in information assurance and this provides the background for students to become future managers. These future mangers will be charged with responsibility for making decisions about the security of information systems. Since there is no 100% secure system and since there are no unlimited budgets to spend on securing systems, choices must be made about how, where and when to invest in security. Students practice methods and techniques for applying industry methodology to problems in information assurance. Mastering this material will make the information assurance professional a better executive. Students develop an understanding of information assurance applied research, executive presentation of topics and financial drivers for budgets and decision making. Students also practice developing and maintaining risk assessments, risk management plans, auditing, and enforcing policies and procedures. Parts of the program are based on the education and training standards of the Committee on National Security Systems certifications CNSS 4012, Senior System Manager (National Security Agency 2013).

 **Hands’ on Experiences through Virtual Labs.** Proprietary virtual lab environments have been developed by program faculty which give students hands’ on experience. One set of labs used in the network and internet security class helps students learn security policy design, incident response, and techniques to defend against, react to, and recover from a cyber-attack. Students conduct comprehensive laboratory exercises on internet protocols, reconnaissance, scanning, vulnerability assessment, and system hardening in a virtual network. These labs are designed with natural relationships among common phases of the attacks and defense technologies, providing students the opportunity to design and implement their own systems that meet a given security policy. Virtual Box is used to emulate the hardware of a computer, and different virtual machines (e.g. Windows XP and Windows 7 virtual machines). These virtual labs enrich students’ experiences in operating and managing various network systems and applications with a minimal operating and maintenance cost.

 Faculty are currently developing a second series of labs that emulate a home computing environment. The main idea is to allow students with little technical experience to practice a series of labs that will develop their cybersecurity skills in a contained environment. Ten labs have been created and many more are in development. Eventually these labs can be used as a training package to help students ensure they have the foundational skills needed to succeed in the program, either before they begin the program or in the first few quarters.

 **Real Business World.** In addition to these elements of the curriculum that link student’s coursework to problems in the real business world, students in the MCL program also benefit from the affiliation with the Business School. In particular, they are able to engage in activities and events that connect them to Masters in Business Administration students and to local private sector employers. For example, students in the MCL program are invited to the annual Professional Networking Event where they learn useful tips on how to build their professional network and engage in several rounds of speed networking. They also are invited to the quarterly Executive Speaker Series where they can benefit from hearing regional business leaders talk about their organizations and experiences. These experiences help to forge informal relationships between students in both programs as well as with private sector employers.

**Institutionalizing Ongoing Engagement between Schools.** Because this is a joint program between two different departments at a university, ongoing administration and governance processes had to be established that can assure continuous learning and improvement. A joint venture between two programs on a campus requires faculty and administration to move beyond their own siloed perspectives and to discover shared areas of interest. A key element for success is the establishment forums for regular dialogue between faculty from the Institute of Technology and the Business School. Quarterly program meetings were established to coordinate and improve the linkages between courses and to discuss students’ progress towards program learning outcomes. New governance vehicles and procedures for managing the curriculum were also established. A committee comprised of faculty teaching in the MCL program is charged with overseeing admissions and developing the curriculum, however votes among each respective faculty are still taken when required by faculty code.

# Technology Conference. Students in the MCL program benefit from the annual Technology Conference, which is hosted by the Institute of Technology, is a technology showcase for the area (Cooper 2013). Since 2000 it has brought together leaders from industry, education and government from around the state to discuss and demonstrate technological innovations and their ongoing applications. The Assistant Director of Industry Partners at the Institute has acted as Co-Chair for the event since 2001 and as Chair since 2004. The Associate Director of the Institute of Technology guides the conference content and has built strong collaborative relationships with business, government and technology partners. Institute undergraduate and graduate students use the conference to showcase their talents and achievement; building networks.

 Panel and keynote presentations - including networking opportunities - provide a venue to discuss, explore, understand and deploy technology as a solution, an opportunity and as an advantage. Sessions planned for the conference have included discussions on mobile application development, energy and sustainability, information technology and cybersecurity. Throughout the conference, graduate and undergraduate students from the Institute of Technology showcase their work through poster sessions and demonstrations in the gallery area. Students get to interact with members of industry and industry participants can observe potential employees in a relaxed atmosphere.

 **Cybersecurity Capstone Challenge.** A capstone is the culminating event for the program. It gives the students an opportunity to apply what they have learned in the classroom and gain valuable job experience and it enables the project sponsors to see the students in action. At the 2013 conference, an open invite was extended for companies and organizations to participate in the Cybersecurity Capstone Challenge. Participants were asked to pose a suitable problem for a team of graduate students to solve in a six month period. The twist is that the potential employers do not get to select the students; instead the students select the project. This reverse job fair makes the companies pose relevant and interesting problems for the students to solve. Benefits to Cybersecurity Capstone Challenge include: giving students the opportunity to apply their cybersecurity studies to real world issues and to receive valuable work experience, giving companies a motivated team at no cost, and enabling both students and company employees to expand their professional networks thus increasing the opportunities to future employment.

 Carving out time for students to work on the capstone is itself a challenge, since many of them work full-time as well as attend class. First, close coordination with each project leader about student constraints and scheduling is essential. Second, take advantage to instructional breaks such as Christmas, Spring Break, and the three weeks between the end of instruction and the final presentation for students to meet with their project leaders. Third, allocate course time to allow for meetings and mentoring.

 A booklet was created that holds the student resumes and the challenges issued by the organizations. The students then met with organizational representatives to ask questions and gain further insight. Students then submitted their preferences on a web form and balanced teams were formed. Teams were developed based on technical skills as well as the ability to write policy. Participants in the challenge include public utilities, software developers, a cybersecurity firm, county level government, and a cybersecurity consultant. Teams are monitored by a faculty member and two cybersecurity consultants. Students periodically report on their project’s progress and are able to hear other teams’ challenges and solutions. An end of year briefing highlights each team’s presentation and marks the conclusion of the program. The masters hooding ceremony follows after a celebration dinner. The richness of the area is reflected in the variety and scope of the cybersecurity challenges listed in table 3.

|  |
| --- |
| 1. Communications Company wants their Unified Communications environment tested against a National Vulnerability Database.
2. An internet security company desires a team to do a controlled assessment inside their Threat Intelligence Lab and link the results to the network defense team.
3. A software company wants to create an approach to embed security in applications development. A second project requests the student team create industry security guidance by assisting a team of developers in writing protocol for emerging technologies.
4. A local county IT department wants a Critical Security Control Audit to evaluate how the county is adhering to Critical Security Controls. The student team will be working with the full-time county team.
5. A local port wants to harden its cybersecurity position based on the NIST Framework. The student team will work in tandem with the port IT staff and other stakeholders.
6. A local utility company desires the establishment of a policy to support the Cybersecurity Framework for Critical Infrastructure.
7. A cybersecurity consulting firm will have a student team work alongside seasoned professionals and be guided in the use of assessment tools, risk analysis, and multiple commercial technologies used with cybersecurity consulting sessions.
 |

Table 3. Cybersecurity Challenges

**Conclusion**

 The MCL is a dynamic and vibrant graduate degree program that serves our local and regional communities by bringing together academia, community leaders, the military, and public and private organizations. This is accomplished through a combination of business and technology related courses and culminates in a capstone project. Through the capstone project, the students interact directly with community partners by applying the knowledge and skills they learned through coursework in practical real-world applications. Stand-alone virtual labs and expert guest speakers supplement the coursework throughout the program. The variety of the students’ professional, military, civic, and academic backgrounds make for rich group collaboration, interaction, debate, and peer review opportunities. The breadth and depth of the security experts brought into the classroom as guest lecturers ensures that students are kept current with the latest advances in the field and are exposed to, and can become a part of, a network of security professionals who can aid them in career advancement. Regular feedback through meetings with students, course evaluations, and faculty discussions, allows program leadership to be responsive to the needs of cybersecurity in general and our students in particular. Being responsive through iterative changes is critical given the dynamic nature of cybersecurity.

**References**

Cooper K. (2013). Hundreds Discuss Mobile Web, Data Security at University of Washington Tacoma’s South Sound Technology Conference (2013). Retrieved from <http://www.tacoma.uw.edu/events/south-sound-technology-conference>

Cybersecurity Forum Initiative - CSFI (2014). Senior Cyber Leadership – Why a Technically Competent Cyber Workforce is Not Enough. Retrieved from <http://www.csfi.us/?page=reports>

George Washington University (2013). Program Requirements of the Master of Cybersecurity in Computer Science. Retrieved from <http://www.cs.gwu.edu/academics/graduate_programs/master/cybersecurity/program-requirements>

Goda, B., Friedman R. (2012). Designing a Masters Program in Cybersecurity and Leadership.

Retrieved from <http://sigite2012.sigite.org/wp-content/uploads/2012/08/session01-paper02.pdf>

Gjelten, T. (2013). Cyber Warrior Shortage Threatens U.S. Security. Retrieved from National Public Radio <http://www.npr.org/templates/story/story.php?storyId=128574055s>

Harris, S. (2012) *Certified Information Systems Security Professional Exam Guide, 6th Edition.* New York. McGraw Hill Professional.

International Information Systems Security Certification Consortium (2014). Certified Information Systems Security Professional. Retrieved from <https://www.isc2.org/CISSP/Default.aspx>

Obama, B. (2009).Obama at the Academy IV: Speech Text. Retrieved from <http://news.sciencemag.org/2009/04/obama-academy-iv-speech-text>.

**Appendix A. Benchmarking Exercise Sources**

National Defense University (2013). Cybersecurity Program. Retrieved from <http://www.ndu.edu/icollege/pcs/pcs_cyberS.html>

National Security Agency (2013). National Information Assurance Training Standard For Senior System Managers. Retrieved from <http://www.scis.nova.edu/documents/cnssi_4012.pdf>

New Jersey Institute of Technology (2013). Master of Science in Cybersecurity and Privacy. Retrieved from <http://cs.njit.edu/academics/graduate/mscsp.php>

University of Maryland (2013). Cybersecurity Education at UMD. Retrieved from

<http://cyber.umd.edu/education>

Utica College (2013). Master of Science in Cybersecurity Online. Retrieved from
<http://programs.online.utica.edu/programs/masters-cybersecurity.asp>

Virginia College (2013). Cybersecurity Master’s. Retrieved from <http://www.vconline.edu/graduate-degrees-online/cyber-security-degree.cfm>

Washington Governor’s University (2013). MS in Information Security and Assurance at WGU. Retrieved from <http://washington.wgu.edu/online_it_degrees/information_security_assurance_degree>

1. Additional graduate programs that combine technical skills with leadership skills that were not included in the original benchmarking exercise include George Mason University’s Management of Secure Information Systems, George Washington University’s World Executive MBA in Cybersecurity, and Washington University’s Cybersecurity Management (c.f., CSFI, 2014). As with the original list, none of these are on the West Coast. [↑](#footnote-ref-1)
2. See Appendix A for a listing of sources from which this data was compiled. [↑](#footnote-ref-2)