NEW PROGRAM PROPOSAL

PRE-APPROVAL FORM

Complete and submit this template when seeking approval *in principle* to move forward with the development of a new programs including: new graduate degrees, diplomas (type 1, 2, or 3), collaborative specializations; new undergraduate degrees, majors, minors, areas of concentration, degree-credit certificates, degree-credit diplomas; major modifications to existing undergraduate programs.

In accordance with the University of Guelph's Institutional Quality Assurance Process (IQAP), all proposed new programs must receive a recommendation to move through the governance process from the Office of the Provost. Submit the completed Pre-Approval Form to either the Director, Academic Programs and Policy (undergraduate proposals) through the Office of Quality Assurance (crc@uoguelph.ca) or the Assistant Vice-President, Graduate Studies (AVPGS) through the Office of Graduate and Postdoctoral Studies (ogps.graduate.curriculum@uoguelph.ca) who, on behalf of the Provost, undertake initial review to ensure new programming is consistent with the strategic plans and directions for growth of the university. Academic units are encouraged to contact the Curriculum Manager in the Office of Quality Assurance or the Manager, Graduate Curriculum in the Office of Graduate and Postdoctoral Studies at the outset of proposal development.

Proposals which include new undergraduate co-op programs must also show evidence the market study is in progress with the Experiential Learning Hub.

Once the sponsoring department/school receives approval in principle, the completed full program proposal must be submitted to the Office of Quality Assurance (undergraduate) or Office of Graduate and Postdoctoral Studies (graduate) within 12 months or the approval will lapse and require resubmission.

Name of Proposed Program(s) and Degree Designation(s):	Master of Cybersecurity Leadership MCSL:L
Sponsoring Department(s)/School(s) and College(s):	School of Computer Science – CEPS Executive Programs - LANG
Proposed Start Date:	Fall 2021
Proposal Lead(s):	Ali Dehghantanha (SoCS) Sean Lyons (LANG)

A. Executive Summary and Brief Program Description

Provide a brief program description and rationale (maximum 1 page) for developing this program. Identify its relationship to the plans of the Department/School and College, the University's Strategic Framework, the Strategic Mandate Agreement (SMA), and existing programs. Include expected program duration and structure, and highlight any potential distinctive curriculum aspects, program innovations, and/or creative components. If known, include proposed experiential learning activities and *ways that issues of equity, diversity, inclusion, and accessibility may be addressed in the proposed program.*

One need only turn on the TV, open a newspaper, or click on a link from a suspicious email to know that cyber crime is on the rise. As the number of computers and IP-enabled devices in homes and businesses grows, as more devices join the Internet of Things, and as the volume and sophistication of cyber attacks and data breaches increase each year, the need for cybersecurity experts with the abilities to protect critical information, assess threats and vulnerabilities, and conduct forensic analysis of cyber incidents will continue to grow. Moreover, there is an existing significant shortage of cybersecurity professionals. In 2014, Cisco Systems estimated a million unfilled security jobs worldwide,[1] and in 2017, Cybersecurity Ventures predicted that there would be 3.5 million unfilled cybersecurity positions by 2021.[2]

In response to this evident trend, the School of Computer Science (SoCS) in collaboration with the Lang School of Business and Economics and University of Guelph's Computing and Communication Services (CCS) proposes a new coursework-based Master of Leadership program in Cybersecurity. On the moral and civic duty to invest in this particular field, Christopher D. Young, CEO of McAfee, LLC, offered the following: "We're approaching a cyber security talent shortage of 2 million people worldwide in the next 3 to 5 years. It's imperative that universities, private companies, and governments join forces to orient today's students toward tomorrow's cyber jobs. Every cybersecurity provider can contribute, and when we're joined by respected education institutions like the University of Guelph, our combined effort makes the world safer."

By working collaboratively, we are able to offer a program that integrates business and leadership acumen with a strong technical background in Cybersecurity. This course-based master's program is targeted at professionals in the cybersecurity field who wish to develop their managerial and leadership competencies, as well as managerial-level professionals who seek to gain a deeper understanding of the techinical aspects of cybersecurity. This professionally oriented 12-month course-based masters will be unique in its core focus on both technical and managerial topics in cybersecurity such as privacy, defence in-depth, security management and audit, threat intelligence, corporate governance and leadership.

The University of Guelph has already invested in the cybersecurity domain by developing a course-based fully technical Master of Cybersecurity and Threat Intelligence (MCTI) program in the SoCS in 2019. The proposed Master of Leadership in Cybersecurity program aims to a target managerial audience and to train the next generation of thought leaders and entrepreneurs in the fast growing field of cybersecurity. Although there are a number of Masters of Business Administration programs in the US and internationally that offer some cybersecurity focus, this program is unique in its dual focus.

This program supports the University's Strategic Framework by:

- **Building knowledge-sharing partnerships –** this inter-disciplinary program will bring together expertise from technical and managerial fields, creating unique opportunities for cross-pollination

[1] Cisco (2014) "Cisco 2014 Annual Security Report," Cisco Systems, www.cisco.com/c/dam/assets/global/UK/pdfs/executive_security/sc-01_casr2014_cte_liq_en.pdf, 60.

[2] Morgan, Steve (May 2017) "Cybersecurity Jobs Report 2018-2021," Cybersecurity Ventures, cybersecurityventures.com/jobs/.

- **Creating innovation in teaching and learning** – an inter-disciplinary degree allows students to interact with colleagues and instructors from varied fields, allowing for emergent learning opportunities
- **Harnessing our strengths, unique capacities and broad interdisciplinary knowledge** – drawing on the expertise of faculty in two colleges and across 3 programs (i.e., Master of Cybersecurity and Threat Intelligence, Master of Leadership, Master of Business Administration), this program provides an exciting opportunity to leverage U of G's unique strengths.
- **Addressing complex questions using comprehensive strengths** – The proposed program draws on the strength of our market-leading Master in Cybersecurity and Threat Intelligence program and the award-winning MBA and MA Leadership program to address a pressing and market-driven demand for cybersecurity managers.

The program supports the Strategic Mandate Agreement by offering a professional program with strong employability potential. The impetus for this program's development was the insistence by industry experts on the Master of Cybersecurity and Threat Intelligence (MCTI) advisory board on the urgent need for greater cybersecurity leadership competencies in the field. The MCTI advisory board includes C-level executives and Chief Information Security Officers of more than 20 companies and government organizations focused on Cybersecurity including Microsoft, IBM, Cisco, Blackberry, McAfee (Intel), RCMP, Canadaian Tire, the Co-Operators. The idea of developing a leadership program in cybersecurity was first highlighted in the MCTI advisory board meeting in Aug 2019 and received overwhelming support including comments from members of the advisory board. This matter was discussed again in the MCTI advisory board meeting of Jan 2021 and many companies on the MCTI board indicated strong interest to support the new master's program with a note that development of this program should be of high priority so that UofG can gain a competitive advantage by being the first mover in this market.

This program is targeted at those who seek to manage the growing cybersecurity workforce. Students may complete the program in one of two ways: (A) course-based option including 8 courses; or (B) project-based option including 6 courses and a Cybersecurity Project. The course work comprises 0.5 credit courses with both a technical and managerial focus. Courses are offered in a mixture of face-to-face and online format.

Option A: Course-based Completion

Four courses [2.0 credits] from School of Computer Science:

- CIS*6510 Cybersecurity and Defence in Depth
- CIS*6550 Privacy, Compliance, and Human Aspects of Cybersecurity
- CIS*65XY Professional Seminar in Cybersecurity (a course that is currently developed for MCTI program)
- CIS*65XY Information Security Management and Governance (a new course dedicated to this program)

Four courses [2.0 credits] from the Lang School:

- MGMT*6200 - Leadership Assessment and Development
- BUS*6850 – Marketing Strategy
- BUS*6180 – Financial and Managerial Accounting
- LEAD*6200 - Leadership of Organizational Change

Option B: Coursework and Cybersecurity Project

Any 3 courses [1.5 credits] selected from each of the lists above (6 in total) and:

- LEAD/CIS*6XXX = Master of Leadership in Cybersecurity Project [1.0 credit]

B. Need and Anticipated Demand

Cybersecurity is a critical function in society and across all sectors of the economy. The number of global cyber-attacks continues to rise, presenting an ever-present and increasing threat to privacy, intellectual property, financial assets and the effective functioning of institutions. Industry demand for cybersecurity professionals is high and will continue to grow. Although technical training in cybersecurity exists, such as the School of Computer Science's Master of Cybersecurity and Threat Intelligence program, there are relatively no existing programs with a focus on the management of cybersecurity strategies and operations.

C. Anticipated Enrolment

Projected enrolment levels for the first 3 years of operation:

Academic Year	Total Enrolment	Year of Program Maturity
2021-2022	25	
2022-2023	35	
2023-2024	40	Yes

The steady-state goal for the program would be one annual cohort of approximately 40 to 50 students (assuming the same tuition fee as the MCTI program) .

D. Resources

This program draws on existing course content from the School of Computer Science and the Lang School of Business. It is necessary to develop an entirely new course titled "Information Security Management and Governance" which specifically focused on delivering the program learning outcomes that are not covered by the existing courses. This course is expected to be delivered by School of Computer Science.

The collaborative nature of the program would allow for the creation of a novel program without the need for any other new courses. The delivery of courses will require the dedication of part of the DOE of faculty from the SoCS (one new teaching task) and one or more departments within LANG. We do not expect the need to hire any new faculty at the School of Computer Science but releasing one undergraduate course allocation from one of the cybersecurity professors to teach the new postgraduate course. As students are either taking projects with industry or take additional courses in the summer we are not expecting a significant change in terms of project supervision for the faculty. However, between this program and existing MCTI program we should have one dedicated postgraduate administrator, one industry liaison officer and 0.5 IT support, and 1 course relief for the director of the program.

The proposed program is expected to be funded through the existing tuition revenue share model for course-based M.Sc. programs. SoCS and LANG plan to evenly split the revenue they receive from central.

SIGNATURES

Signatures confirm receipt, review, and approval *in principle* of the proposed new program.

For expediency, it is recommended that Proposal Leads secure the signatures of the Department Chair/Director and College Associate Dean prior to submission to the Office of Quality Assurance or Office of Graduate and Postdoctoral Studies.

Department Chair(s)/Director(s) *Date*

College Associate Dean Research and Graduate Studies or Associate Dean, Academic *Date*

Executive Director, Budget and Financial Planning *Date*

Assistant Vice-President, Institutional Analysis and Research *Date*

Assistant Vice-President, Graduate Studies or Associate Vice-President (Academic) *Date*