Ryerson University

Graduate Studies

Letter of Intent

Cybersecurity and Information Assurance (MSc, MCIA)

Submitted to YSGS: March 25, 2020

Last Updated: January 25, 2021

TABLE OF CONTENTS

NEW GRADUATE PROGRAM – LETTER OF INTENT (LOI)

1.1 Degree Name and Description

This document proposes to add a **Master of Science in Cybersecurity and Information Assurance (MSCIA)**, a thesis-based two-year master's program, and a **Master of Cybersecurity and Information Assurance (MCIA)**, a one-year course-based master's program with a capstone option. These programs are new, interdisciplinary graduate programs balancing both technical aspects of cybersecurity as well as managerial aspects of information assurance. They are innovative programs, combining the considerable strengths of Ryerson's faculty in computer science, IT management, and electrical and computer engineering.

Identification of Designated Academic Unit

The program will be interdisciplinary and housed within Yeates School of Graduate Studies (YSGS).

Program Governance Structure

The program would be directed by a Graduate Program Director and administered by a full-time Graduate Program Administrator. The Dean of Record will be the Vice-Provost and Dean, YSGS. The program would be governed by a Graduate Program Council (GPC) that will be developed according to Senate Policy 45. It will include the GPD, faculty members actively involved in the program and graduate student representatives. The GPC reports directly to the YSGS Council. A Board would be created to continuously oversee the resourcing of the program (both physical and human). The Board would consist of the Deans or designates from the Faculty of Science (FOS), Faculty of Engineering and Architecture (FEAS) and the Ted Rogers School of Management (TRSM), the Chairs/Directors of the Department of Computer Science, the Department of Electrical, Computer and Biomedical Engineering, and the School of Information Technology Management, and the Director of the proposed program. The inaugural graduate program director is Dr. Atefeh Mashatan, who led the development of this LOI.

Principal Faculty Involved in the Proposal Development

This letter of intent (LOI) has been developed by Atefeh Mashatan, director of the Cybersecurity Research Lab and assistant professor of Information Technology Management in collaboration with a working group consisting of Charles Finlay, executive director of Rogers Cybersecure Catalyst; Alex Ferworn, professor of Computer Science; Ali Miri, professor of Computer Science; Avner Levin, professor of Law; Bouchaib Bahli, professor of Information Technology Management; and Muhammad Jaseemuddin, Professor of Electrical, Computer and Biomedical Engineering and Program Director, Computer Networks Master of Engineering. The LOI was reviewed by Cory Searcy, the Dean of Record; David Cramb, Dean of the Faculty of Science; Daphne Taras, Dean of the Ted Rogers School of Management (TRSM); Thomas Duever, Dean of Faculty of Engineering and Architectural Science; Carl Kumaradas, Associate Dean, Programs in YSGS;

1.2 Overlap/Integration with other Programs

As a standalone program housed in YSGS and devised in collaboration with the Ted Rogers School of Information Technology Management (TRS-ITM), the Department of Computer Science in the Faculty of Science (FOS-CS) and Electrical, and the Department of Electrical, Computer, and Biomedical Engineering in the Faculty of Engineering and Architectural Science (FEAS-ECBE), this master's program is unique at Ryerson. It offers a multidisciplinary learning experience, providing students with an integrated framework for dealing with cyber threats, risks, and vulnerabilities from both technical and business perspectives. The program is based on the knowledge that hardware and software solutions alone are not sufficient: organizations need

well-rounded cybersecurity professionals who are able to understand and assess the business context of cyber risk. For instance, a managerial background will help a cybersecurity professional assess and size the business risk and which types of threats are most dangerous to an organization, where and how data should be stored, and how much access each employee should be granted to sensitive information. Only with an understanding of an organization's industry, structure, and assets can a professional accurately assess how much danger any given threat poses, and how to protect against it.

In order to ensure that the graduates obtain both managerial and technical proficiency, the program will draw faculty members from TRS-ITM, FOS-CS and the department of Electrical and Computer Engineering in the Faculty of Engineering and Architectural Science (FEAS-ECE) to teach courses and supervise capstone projects and theses.

Existing master's-level programs related to the disciplines of cybersecurity and information assurance include the FOS's MSc in Computer Science, FEAS's MASc and MEng in Computer Networks, and TRSM's MSc in Management. Students in all three faculties can do thesis work on cybersecurity when supervised by a professor who has the expertise, but there is no substantial coursework on the subject that prepares the students for the job market or further graduate studies in cybersecurity or information assurance. The proposed master's program will provide students with a much greater depth of knowledge of the field, and it will also teach students with technical backgrounds about managerial issues, and vice versa. Representing a collaboration between three faculties at the graduate level—something unique at Ryerson—the program will be poised to attract a range of students wishing to gain a well-rounded graduate education in the field.

At the undergraduate level, Ryerson is currently developing a minor in Cyber Studies, to be offered within the Faculty of Science. Students in the proposed master's program will acquire a considerably greater depth and breadth of knowledge than those taking the minor; however, the minor will help to illustrate how the master's program is an important part of a continuum of cybersecurity learning at Ryerson.

This continuum may in the future be enhanced by a full BSc in Cybersecurity and/or a BComm in Information Assurance. Indeed, such degrees could provide an ideal pipeline for students to enter the MSc in Cybersecurity and Information Assurance program.

1.3 Program Details

The program will bolster Ryerson's status in cybersecurity education, addressing a national and global need for cybersecurity professionals trained in the technical and managerial aspects of cybersecurity. It will also encourage the production of research addressing evolving cyber threats with a holistic approach drawn from both disciplines.

The program is clearly aligned with the university's plans, as it addresses themes and priorities articulated in Ryerson's *Academic Plan 2020–25* and *2020–25 Strategic Research Plan*.

1.3.1 Alignment with University's Plans

Cybersecurity

The *2020–25 Strategic Research Plan* highlights cybersecurity as an "immediate global issue" and lists it as an area of focus. The university has committed itself to leveraging "both resources and entrepreneurial capacities to solve critical security challenges."

These challenges are widespread, multifaceted, and rapidly evolving. The MSCIA and MCIA programs will enable Ryerson to address them more effectively, training experts to tackle these challenges in holistic ways. The strategic research plan also identifies Future Skills as an area of focus, highlighting the "changing nature of skills and competencies," and the proposed MSc program will be attentive to how these changes are occurring and how cybersecurity professionals can keep pace. Furthermore, the program will promote the production of original research that takes into account cybersecurity's technical and managerial dimensions. By doing so, the program will complement the existing work of Rogers Cybersecure Catalyst and the Cybersecurity Research Lab. It will further Ryerson's commitment to excellence while elevating the university's reputation as a leader in cybersecurity—which in turn will enable Ryerson to attract more internal and external graduate students.

Innovation

Cybersecurity is essential to fostering innovation, which is one of the priorities listed in the *Academic Plan 2020–25*. In its 2017 report *The CEO's Guide to Data Security*, AT&T warned that the immensity of the threat posed by cybercrime "risks the incentives for innovation and investment." Thus, the experts trained in this MSc program will play a significant role in safeguarding technological innovation itself. Furthermore, Technology & Intelligent Systems is one of the strategic themes identified in the *2020–25 Strategic Research Plan*, which stresses how Ryerson, working with industrial partners, "is creating a strong technological and industrial ecosystem." That ecosystem can only be maintained with a robust commitment to cybersecurity.

New Partnerships

Another priority listed in the academic plan is Scholarly, Research, and Creative Activity and Graduate Studies, which acknowledges the way "new partnerships and endeavours, based on our talent and research expertise, promise to deepen our research intensity and overall influence." A third priority in the plan, Community and Urban Partnerships, also stresses the need to collaborate "with experts from other cities and institutions to share learning, ideas and solutions on critical urban issues." The program's proposed areas of study and focus have been developed in consultation with numerous Chief Information Security Officers (CISOs) and Chief Security Officers (CSOs) of Canadian corporations, all of them based in major Canadian cities, to ensure they can readily be applied in real-world situations, thus furthering Ryerson's promotion of applied—and applicable—research. Moreover, this MSc program will be attractive to industry partners looking to hire much-needed industry-ready graduates.

City-Building

In its discussion of the Community and Urban Partnerships priority, the academic plan stresses the importance of a "focus on city-building" and "enhancing our expertise as a leader in urban scholarship and research." Moreover, City Building and Urban Innovation is an area of focus in the strategic research plan. The concept of city-building refers not only to the literal built environment, but also to its social and economic foundations. There is a significant, well-established talent shortage in cybersecurity, demonstrated, for example, by the 2019 Cybersecurity Workforce Study by the International Information System Security Certification Consortium, or $(ISC)^2$, an international association of certified cybersecurity professionals, which shows a global gap of over 4 million professionals. This shortage threatens to destabilize the aforementioned foundations of Canadian cities, and the MSc program will play an important part in reinforcing them.

Inclusion

The academic plan lists Equity, Diversity, and Inclusion as one of Ryerson's values, recognizing equity and

diversity as "essential components of a modern, accessible post-secondary institution." This commitment is especially important given the well-established lack of equity and diversity in the field of cybersecurity. The latest (ISC^2) Cybersecurity Workforce Study (from 2019) has found that "Cybersecurity professionals are more than twice as likely to be male," and Lisa Kearney, CEO of the organization Women Cybersecurity Society, was quoted in February 2020 as saying women account for only 10% of the Canadian cybersecurity workforce. (ISC^2)'s 2017 white paper "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce" has found that in the United States, women and minorities are underrepresented in leadership roles and trail their white male counterparts in average salary.

As a collaboration between the faculties of science and management, the program would be poised to welcome a generally more diverse student body than technically focused cybersecurity programs: There is more diversity among the pool of undergraduates with management degrees, and among people with management expertise, than among those with computer science education and expertise.

Moreover, a fourth priority listed in the academic plan is The Student Experience, which calls for "the creation of accessible, inclusive and engaging learning environments for a diverse student population." The proposed MSc program will welcome a diverse roster of guest speakers from industry who will be able to relate their experiences in the field. In addition, the program will be working with industry partners, many of whom will be eager to help students from underrepresented communities see a pathway to success. The program will also be part of a cybersecurity ecosystem at Ryerson that fosters diversity, as typified by Cyber Catalyst's Accelerated Cybersecurity Training Program for women, new Canadians, and displaced workers.

Appropriateness of Degree Nomenclature

As demonstrated in section 1.4.3, there are many graduate programs in cybersecurity and related fields whose names do not accurately or clearly reflect their areas of focus. The title of these programs, i.e., cybersecurity and information assurance, is appropriate because of the program's equal focus on two areas, and because it adheres to accepted definitions of both disciplines: cybersecurity as a technical field involving securing data, and information assurance as a managerial field involving devising policy and managing risks within an organization.

1.3.2 Learning Outcomes and GDLEs

The Master of Cybersecurity and Information Assurance seeks to produce graduates who have a mastery of both the business and technical aspects of cybersecurity and who will be well placed to supervise all aspects of an organization's cybersecurity program as part of its larger business goals.

The proposed program's overall aim is to foster an environment where students are well-rounded and possess the agility and expertise required to mediate between business and technical contexts.

The following are the program's ten learning outcomes (LOs). Upon completion of this program, graduates will be able to:

1. Discuss both the business and technical aspects of cybersecurity, as well as their interrelation.

2. Describe and demonstrate the value of a holistic approach derived from business and technology to an organization's cybersecurity program.

3. Analyze the evolving role of cybersecurity professionals in terms of the field's historical context.

4. Assess and analyze internal and external cybersecurity risks. Assess an organization's security program using GRC (governance, risk, and compliance) concepts and their associated frameworks.

    - Identify, assess, and analyze the probability and impact of cyber threats to an organization (Cybersecurity Risk Management).
    - Identify internal and external cybersecurity risks to an organization (Cybersecurity Risk Management).
    - Recommend IT risk management solutions to organizations, and implement them (Cybersecurity Frameworks, Governance, and Compliance).
    - Evaluate an organization's compliance with industry and regional cybersecurity regulations (Cybersecurity Frameworks, Governance, and Compliance).
5. Demonstrate a thorough understanding of the fundamentals of security technologies.
    - Assess and bolster an organization's identity and access management (IAM) and to protect its data (Fundamentals of Security Technologies).
    - Explain the information security principles underlying an organization's architecture system (Security Architecture).
    - Apply logical security architecture to help an organization achieve its information security and privacy goals (Security Architecture).

6. Communicate effectively with and across management and technical teams.

Mapping the Program Learning Outcomes against the Masters GDLEs

TABLE 1: Comparison of learning outcomes to Graduate Degree-Level Expectations (GDLEs)

GDLE	**Master of Science Degree** *This degree is awarded to students who have demonstrated:*	**Master of Cybersecurity and Information Assurance:** Program Learning Outcomes addressing each GDLE
1. Depth and breadth of knowledge	A systematic understanding of knowledge, including, where appropriate, relevant knowledge outside the field and/or discipline, and a critical awareness of current problems and/or new insights, much of which are at, or informed by, the forefront of their academic discipline, field of study, or area of professional practice.	LO1, LO2, LO3, LO4, LO5
2. Research and scholarship	A conceptual understanding and methodological competence that: enables a working comprehension of how established techniques of research and inquiry are used to create and interpret knowledge in the discipline;	LO3, LO4, LO5, LO6
	enables a critical evaluation of current research and advanced research and scholarship in the discipline or area of professional competence;	LO4, LO5, LO6
	enables a treatment of complex issues and judgments based on established principles and techniques; and,	LO4, LO5, LO6
	on the basis of that competence, has shown at least one of the following: development and support of a sustained argument in written form; OR originality in the application of knowledge.	LO4, LO5
3. Level of Application of knowledge	Competence in the research process by applying an existing body of knowledge in the critical analysis of a new question or of a specific problem or issue in a new setting. Exposure to technology solutions and toolset in lab settings.	LO4, LO5
4. Professional Capacity /Autonomy	The qualities and transferable skills necessary for employment requiring: The exercise of initiative and of personal responsibility and accountability; and Decision-making in complex situations; and	LO4, LO5
	The intellectual independence required for continuing professional development;	LO4, LO5
	The ethical behaviour consistent with academic integrity and the use of appropriate guidelines and procedures for responsible conduct of research; and	LO5
	The ability to appreciate the broader implications of applying knowledge to particular contexts.	LO1, LO2, LO4, LO5

5. Communication skills	The ability to communicate ideas, issues and conclusions clearly.	LO1, LO6
6. Awareness of limits of knowledge	Cognizance of the complexity of knowledge and of the potential contributions of other interpretations, methods, and disciplines.	LO1, LO2, LO3

Taken together, all four core courses (Cybersecurity Risk Management; Cybersecurity Framework, Governance and Compliance; Fundamentals of Security Technologies; and Security Architecture) address the 6 learning outcomes. Please see 1.6.2 for further details.

1.4 Societal Need

Our interconnected 21st-century way of life depends on cybersecurity. It is vital to everything from our personal privacy to the reliability of our banking system to the safe delivery of medical care to the integrity of our elections. It safeguards our economy and our democracy.

As outlined in section 1.3.1, there is a significant shortage of trained cybersecurity workers in Canada and around the world. In particular, there is a need for workers who have a breadth and depth of knowledge of both technical and managerial aspects of cybersecurity.

Cybersecurity is a priority for the federal government, which has noted in its National Cyber Security Action Plan (2019-2024) that cybercrime costs the country $3 billion per year. In January 2020, Minister of Innovation, Science and Industry Navdeep Bains announced an Intelligence and Cyber Centre in Vancouver, designed to "make Canada a leader in cybersecurity."

Currently, Canada lags behind the United States in postgraduate cybersecurity education: Cybercrime Magazine's "2020 Directory Of M.S. In Cybersecurity Programs At Universities In The US," which is not exhaustive, lists 188 such programs. Given that the US has over nine times Canada's population, one would expect at least 20 such programs in Canada; however, there are far fewer. Please see section 1.4.3 for details.

The proposed master's program could play an important role in helping Canada fulfil its aim to become a cybersecurity leader.

1.4.1 Labour Market

An influential business report by Cybersecurity Ventures, sponsored by Herjavec Group and reported on by the New York Times, calls cybercrime "the greatest threat to every company in the world," predicting that by 2021, its global annual cost will be more than $6 trillion [US].

Contributing to this astonishing figure is a significant gap between demand and supply in the workforce. A November 2019 study by (ISC^2) found that globally, there is a need for 4.07 million professionals to close the skills gap in cybersecurity.

The same study found that Canada's cybersecurity workforce consists of approximately 84,000 people, and that the cybersecurity workforce gap in North America is approximately 561,000. $(ISC)^2$ has calculated that the gap in the United States alone is "nearly 500,000," which leaves a shortage of approximately 61,000 professionals in Canada and Mexico (the other two North American countries included in the study). Mexico's

cybersecurity workforce is listed as 341,000—approximately four times Canada's workforce. Assuming the demand in Mexico is four times that in Canada, we may estimate a gap of roughly 12,200 in Canada.

Many of these professionals will be required in Ontario, and especially in the Greater Toronto Area. On the website LinkedIn.com alone, a search for cyber security jobs on March 24, 2020 revealed 1787 positions in Canada, of which 802 (44.9%) were in Ontario and 479 (26.8%) in the Greater Toronto Area. Ryerson's campus-based MSc is therefore well-placed to help address this local and provincial shortage.

There is a 0% unemployment rate for cybersecurity professionals, and Ryerson's MSc in Cybersecurity and Information Assurance graduates will be industry-ready. Moreover, in addition to the multidisciplinary training they will receive, they will benefit from how the program is structured. Graduates will be able to demonstrate thorough familiarity with the Common Bodies of Knowledge required for the Certified Information Systems Security Professional (CISSP) program offered by $(ISC)^2$ and will thus be ready to pass the exam for this certification. The certification is relevant to both technical practitioners and managers, and it is globally accepted and recognized. According to the international IT training company Global Knowledge, is currently the sixth-best IT certification overall for 2020. Therefore, graduates will be attractive to organizations for mid-level positions as opposed to the common entry-level positions filled by graduates from undergraduate programs.

1.4.2 Student Demand

Given the national and global shortage of cybersecurity professionals, it is no surprise that Deloitte's report "The Changing Faces of Cybersecurity – Closing the Cyber Risk Gap" identifies high student demand in Canadian universities for "cybersecurity programming at both the undergraduate and graduate levels." It also notes that "Industry perceives a lack of focus on training cybersecurity graduates who can make an immediate contribution to the business."

The MSCIA's connection with the Ted Rogers School of Management, as well as the connections the program will forge with industry partners, will make the program especially relevant to industry—a strong selling point for prospective applicants.

Moreover, Ryerson's growing reputation as a hub for cybersecurity research, innovation, and training—with Rogers Cybersecure Catalyst, the Cybersecurity Research Lab, and the Privacy and Big Data Institute all playing important, high-profile-roles—will be attractive to students wanting to study at an institution that is a cybersecurity leader.

The cybersecurity education Ryerson offers is already in high demand: for example, Cyber Catalyst has received 20 applicants for every spot available in the second cohort of its cybersecurity training program. Although this is not a comparator program for a graduate degree, it speaks to the market need and student demand.

Moreover, the MSCIA program will be attractive to graduates of Ryerson's own programs, including graduates with a BSc in Computer Science who wish to learn about the managerial aspects of cybersecurity and BComm graduates who wish to learn about the field's technical aspects.

The program will also be able to draw on the large number of IT and financial services workers in the Greater Toronto Area who wish to upgrade their credentials and become more well-rounded applicants for positions with greater responsibilities and higher pay. The program will also be attractive to recent graduates of other GTA and southern Ontario universities who wish to continue to live in the area.

Anticipated Enrolment

The proposed program will be full-time only. We anticipate an intake of 18-24 students per year: 3-4 in the thesis pathway, 6-8 in the capstone pathway, and 9-12 in the course-based pathway. There will therefore be a maximum of 28 students (24 first-year + 4 second-year thesis) in the program at the same time.

Class sizes will therefore range from 18 to 24 in the core courses; electives will be considerably smaller.

While student demand is likely to be high, in order to further Ryerson's commitment to excellence in quality education, we are committed to keeping class sizes small enough to provide for productive mentor-mentee relationships between faculty and students.

1.4.3 Comparator Programs

The following section addresses comparator programs offered by Canadian and American universities (including two offered in Canada).

Canadian Universities (please see Table 2)

There are only two master's programs in cybersecurity offered by Canadian universities: the University of Guelph's Master of Cybersecurity and Threat Intelligence, and the University of New Brunswick's Master of Applied Cybersecurity. Both are one-year programs primarily focused on the technical aspects of cybersecurity.

In Quebec, Concordia University offers an exclusively computer science-focused Master of Applied Science (MASc) of Information Systems Security.

Ontario Tech University began a two-year Master of Information Technology Security program in 2018; although it includes two core courses covering the areas of law, ethics, security policy, and risk management, it is primarily technology-based putting more emphasis on technical content on all its other courses and being taught in a technical department.

In Alberta, Concordia University of Edmonton offers both a business-focused Master of Information Systems Assurance Management and a Master of Information Systems Security Management, the latter of which offers both technical and managerial courses related to information security. The program, however, is a management degree (rather than a Master of Science) run through the university's faculty of management, taking up at least 20 months of full-time study, and it does not offer a thesis option.

US Universities with Canadian Campuses (please see Table 3)

Two US universities that have Canadian campuses offer Master of Science (MS) in Cybersecurity programs. The New York Institute of Technology offers an MS in Cybersecurity at its Vancouver campus; this is an entirely technology-based program. Northeastern University Toronto's MS program is structured around a technical track and a "contextual" track that focuses on legal and managerial issues; students must take two courses from each track, as well as a foundation course on information assurance and electives. The program's integration of management and technical streams is itself similar to Ryerson's; however, the management courses are taught through a US lens that addresses federal and state laws, resources, and programs. Moreover, as of the 2018–19 school year, the program had only two full-time faculty on the Toronto campus, with certain courses available only online to students in Toronto; moreover, the program did not have the ability to bring in international students or offer OSAP funding.

US Universities with US Campuses or Online-Only Programs (please see Table 4)

The many MS programs in Cybersecurity are largely divided between business school-based and computer engineering/computer science-based programs. Some universities offer both types of degree (e.g., Iowa State, New York University, University of New Hampshire, Carnegie Mellon). Others offer a single degree (MS in Cybersecurity) with different concentrations, for example Georgia Tech (technology, cyber-physical, public policy), De Paul University (networking and infrastructure; computer security; governance, risk management and compliance), University of Delaware (secure software, secure systems, security analytics, security management), and Villanova University (systems, policy, operations). With so few electives required, these programs, with their concentrations, do not realistically replicate the truly multidisciplinary nature of Ryerson's holistic MSc in Cybersecurity and Information Assurance.

However, some institutions in the United States do offer multidisciplinary programs, including some of the country's most reputable colleges and universities. The University of Indiana offers an MS in Cybersecurity Risk Management that obliges students to take courses in managerial, technical, and legal aspects of the field. The University of Berkeley, California offers an online-only Master of Information and Cybersecurity that is advertised as developing "students' understanding of information security technologies as well as the economic, legal, behavioral, and ethical impacts of cybersecurity." Northeastern's interdisciplinary MS as offered at its Boston campus is much more established than its Toronto version.

There are significant differences between these programs and Ryerson's proposed program—Berkeley's is not a Master of Science; the University of Indiana obliges students to take courses specifically relevant to American (not Canadian) law, and Northeastern also has US-focused coursework. Nonetheless, the fact remains that these and a handful of other US-based programs have recognized the value of combining managerial and technical knowledge to produce well-rounded graduates.

The Proposed MSCIA in Context

Although the proposed master's program will not be the first in North America to derive a holistic approach to cybersecurity from managerial and technical streams, it will serve an important purpose, particularly for Canadian students and those wishing to work in Canada.

Ryerson will be the first Canadian public research university to offer such a program. Moreover, its MSc, drawing on faculty from TRS-ITM, FOS-CS and FEAS-ECE, will have access to a much more robust set of resources than the interdisciplinary programs at Concordia University of Edmonton and Northeastern's Toronto campus.

In contrast to many of the US-based cybersecurity programs, it offers in-person instruction and does not oblige students to study material that is specific to US law and regulations. Moreover, in contrast to the US-based programs cited in Table 4, it offers a course-based pathway that can be completed in one academic year, and which is particularly suitable for students wishing to enter (or re-enter) the job market quickly.

TABLE 2: Canadian universities

Institution	Degree offered	Required courses	Disciplinary lens	Type (course-based, project- based or thesis-based)	Campus or online	Duration
Concordia University (School of Engineering and Computer Science)	Information Systems Security, Master of Applied Science (MASc)	20 credits (16 required), thesis (co-op option) INSE 6110 Foundations of Cryptography INSE 6120 Crypto-Protocol and Network Security INSE 6130 Operating Systems Security INSE 6140 Malware Defenses and Application Security	tech	thesis	campus	18–24 months
Concordia University of Edmonton (Faculty of Management)	Master of Information Systems Security Management	13 required courses, 1 elective, 2 research courses ISSM 521 TCP/IP Security ISSM 525 Securing an E-Commerce Infrastructure ISSM 531 Advanced Network Security ISSM 533 Cryptography and Secure Network Communications ISSM 535 Firewall Fundamentals ISSM 536 Digital Forensics ISSM 538 Research Methods I ISSM 541 Management Accounting ISSM 543 Systems Development and Project Management ISSM 545 Security Policies, Standards and Management ISSM 551 Disaster Recovery and Planning ISSM 553 Governance, Risk and Control	hybrid	2 research courses	campus	2 years

		ISSM 561 Information Technology Law and Ethics				
Concordia University of Edmonton (Faculty of Management)	Master of Information Systems Assurance Management	60 credits, including 14 mandatory courses (half from the ISSM program), 2 electives, 2 research projects ISAM 512 Financial Accounting, Governance and Assurance ISAM 521 Information Systems Audit I ISAM 522 Information Systems Audit II ISAM 542 Fraud Examination: Theories and Methods ISAM 549 Auditing Theory and Application ISAM 558 Research Methods II ISAM 581 Research Project in Subject Area ISSM 541 Management Accounting ISSM 543 Systems Development and Project Management ISSM 521 TCP/IP Security ISSM 545 Security Policies, Standards and Management ISSM 551 Disaster Planning and Recovery ISSM 538 Research Methods I ISSM 553 Risk Management	business	2 research projects	campus	2 years
University of Guelph (School of Computer Science)	Master of Cybersecurity & Threat Intelligence	4.0 graduate credits, consisting of 5 core courses (0.5), one elective course (0.5) and an independent project (1.0) in partnership with an academic or industry expert CIS*6510 Cyber Security and Defence in Depth	tech	research project	campus	1 year

		CIS*6520 Advanced Digital Forensics and Incident Response CIS*6530 Cyber Threat Intelligence and Adversarial Risk Analysis CIS*6540 Advanced Penetration Testing and Exploit Development CIS*6550 Privacy, Compliance, and Human Aspects of Cybersecurity				
University of New Brunswick (Faculty of Computer Science)	Master of Applied Cybersecurity	INFO2403 Fundamentals of Information Security (only if this prerequisite is missing) CS6865 Advanced Data Communications and Networking CS6411 Fundamentals of Information Assurance CS6355 Cryptanalysis and Database Security CS6415 Network Security CS6413 Foundations of Privacy CS6417 Software Security One course from (CS6075, CS6585, CS6735, TME3423, TME6386, MBA6606) CS6419 Digital Forensics CS6495 Capstone Project	tech	capstone R&D project defined by industry	campus	1 year
Ontario Tech University (Faculty of Business and Information Technology)	Master of Information Technology Security	30 credits (24 required courses) + either two Capstone Research Projects, or 2 electives in IT security or relevant topics, or an internship MITS 5100G Law & Ethics of IT Security MITS 5400G Secure Software Systems MITS 5500G Cryptography and Secure Communications	tech	courses, capstone, or internship	campus	2 years

		MITS 6400G Biometrics/Access Control and Smart Card Technology MITS 5200G Advanced Communication Networks MITS 5300G Operating Systems Security MITS 5600G Security Policies and Risk Management MITS 6100G Attack and Defence MITS 5900G MITS Seminar (0 credit)				

TABLE 3: US universities with Canadian campuses

Institution	**Degree offered**	**Required courses**	**Disciplinary lens**	**Type (course-based, project- based or thesis-based)**	**Campus or online**	**Duration**
Northeastern University Toronto (Khoury College of Computer Sciences)	Master of Science in Cybersecurity	32 semester hours:1 foundation course (4 hours); 2 courses (4 hours each) from both the contextual and technical tracks (16 hours); 2 electives (4 hours each); 1 capstone project (8 hours) CY 5010 Foundations of Information Assurance Technical Track CY 5120 Applied Cryptography CY 5130 Computer System Security CY 5150 Network Security Practices CY 6120 Software Security Practices Contextual Track CY 5200 Security Risk Management and Assessment CY 5210 Information System Forensics CY 5240 Cyberlaw: Privacy, Ethics, and Digital Rights	hybrid	capstone project	online, campus, hybrid	18–24 months

		CY 5250 Decision Making for Critical Infrastructure Capstone CY 7900 Capstone Project				
New York Institute of Technology, Vancouver campus	MS in Cybersecurity	30 credits: 24 credits from required courses + 6 credits of electives (Vancouver campus curriculum requirements, listed here, are more limited than at the other campuses, e.g., no thesis option, more required courses, fewer electives) Information, Network, and Computer Security CSCI 620 Operating System Security CSCI 651 Algorithm Concepts INCS 618 Computer Security Risk Management and Legal Issues Computer Security INCS 615 Network Security and Perimeter Protection INCS 741 Cryptography INCS 745 Intrusion Detection and Hacker Exploits Required in Vancouver only: INCS 712 Computer Forensics INCS 775 Data Center Security	tech	course-based (Vancouver campus only)	?	variable

TABLE 4: Selected US universities with similar courses (MS programs only)

Institution	Degree offered	Required courses	Disciplinary lens	Type (course-based, project- based or thesis-based)	Campus or online	Duration
Capitol Tech University	MS in Cybersecurity	36–39 credits; 24–27 core, + 12 electives from IA or project management IAE-500 Introduction to Information Assurance CS-620 Operating System Principles for Information Assurance [waivable] IAE-671 Legal Aspects of Computer Security and Information Privacy IAE-675 Computer Forensics and Incident Handling IAE-677 Malicious Software IAE-679 Vulnerability Mitigation IAE-680 Perimeter Protection IAE-682 Internal Protection IAE-685 Principles of Cyber Security IAE-674 Security Risk Management	hybrid (tech-leaning)	course-based	online	variable
Dakota State University	Masters of Science in Cyber Defense	30 hours: 8 core courses + 2 electives INFA 701 - Principles of Information Assurance INFA 713 - Managing Security Risks INFA 720 - Incident Response INFA 721 - Computer Forensics INFA 723 - Cryptography INFA 735 - Offensive Security INFA 751 - Wireless Security INFA 754 - Intrusion Detection	hybrid	course-based	online	2 years

University of Detroit Mercy	Master of Science in Information Assurance with a major in Cybersecurity	CYBE 5700 Principles of Cybersecurity (3 credits) CYBE 5730 Cyberlaw (3 credits) CYBE 5740 Secure Acquisition (3 credits) CYBE 5750 Cybersecurity Technologies (3 credits) CYBE 5770 Cyber Defense Operations (3 credits) CYBE 5780 Risk Management Processes (3 credits) CYBE 5790 Cybersecurity Control Processes (3 credits) CYBE 5910 Information Audit (3 credits)	hybrid	course-based	online	variable
George Mason University	Management of Secure Information Systems MS	36 credits required courses MSEC 510 Foundations of Cyber Security MSEC 511 Security Practices in the Enterprise MSEC 520 Networking Principles MSEC 620 Networking Security MSEC 630 Secure Information System Governance, Regulation, and Compliance MSEC 641 Enterprise Security Threats MSEC 642 Enterprise Security Technologies MSEC 650 Seminar: Enterprise Security Case Studies PUBP 610 Organizations, Management, and Work: Theory and Practice PUBP 611 Critical Infrastructure Protection in Theory, Policy and Practice MSIS 611 Leadership and Change Management	hybrid (business leaning)	capstone	campus	16 months

		MSIS 614 Financial and Cost Accounting MSIS 620 Economics of Technology Management MSIS 635 Decision Models and Methods MSIS 643 Managerial Finance MSIS 747 Enterprise Information Security Audit MSIS 735 Capstone Project or MSEC 720 Capstone Project in Management of Secure Information Systems MSIS 750 Global Practices in Security of Information Systems or MSEC 710 Global Residency				
Indiana University	MS in Cybersecurity Risk Management	6 credit hours in each of the following areas: ● Technical cybersecurity ● Information technology risk management ● Cybersecurity law and policy 9 credit hours electives	interdisciplinary; stream focussed	capstone	online, campus, hybrid	variable
Lewis University	MS in Information Security	CPSC-50000 Computer Organization CPSC-50100 Programming Fundamentals INSY-50500 Introduction to Information Security INSY-51000 Business Data Networking CPSC-51500 Operating Systems CPSC-52000 Network Security Essentials CPSC-52500 Encryption and Authentication INSY-53000 Legal & Ethical Issues in Information Security	hybrid (with technical and managerial concentrations)	capstone	online, campus, hybrid	Part-time only (must be completed within 7 years)
Walden University	MS in Cybersecurity	10 required courses	hybrid	none	online	84 weeks

		CSEC 6005 The Global Technology Environment CSEC 6215 Security Risk Management CSEC 6210 Cloud Computing CSEC 6175 Software Testing and Quality Assurance CSEC 6190 Foundations of Intelligent Systems CSEC 6670 Security Engineering and Compliance CSEC 6735 Applied Cryptography CSEC 6270 Cyber Forensics CSEC 6255 Cybercrime Prevention and Protection CSEC 6635 Secure Coding				
Western Governors University	Master of Science Cybersecurity and Information Assurance	30 hours, all required Information Security and Assurance Secure Software Design Cybersecurity Architecture and Engineering Cybersecurity Management I - Strategic Ethical Hacking Cybersecurity Management II - Tactical Forensics and Network Intrusion Secure Network Design Cybersecurity Graduate Capstone	hybrid	capstone	online	2 years

1.5 Admission Requirements

The program-specific admission requirements for the Master of Science in Cybersecurity and Information Assurance are drawn from the admission requirements of the Master of Computer Science and Master of Science in Management.

- Completion of a four-year Bachelor's degree from a recognized institution in a related field (e.g.,

computer science, business technology management, computer engineering, electrical engineering), with a 3.0 GPA, or above" in the last two years of study, including post-graduate university programs.

- Applicants who have not completed two or more years of full-time postsecondary education at a Canadian university or a university at which English was the primary language of instruction must provide proof of language proficiency, as per the graduate school English Language Requirements listed here: https://www.ryerson.ca/graduate/future-students/apply/requirements/
- Two letters of recommendation, at least one of which must be from a former postsecondary instructor; the second may be academic or professional.
- A research statement of approximately 500 words that includes:
    - Outline of reasons for applying to the MSCIA program, including career objectives,
    - Any sources of funding held or applied for to support graduate studies (scholarships, fellowships, grants, awards, self-funding, etc.).

  If the applicant wishes to pursue the thesis option, the following should also be included in the research statement:
    - Research interests/plan that the applicant wishes to pursue as a possible thesis topic while in the program,
    - Explanation of how previous studies and experiences have shaped those research interests,
    - Identification of at least two to three potential supervisors and an explanation as to why the faculty members chosen would make a good supervisor for the applicant's research.

1.5.1 Program Learning Outcomes

The admission requirements are appropriate for the learning outcomes as they ensure that potential students will have the academic, research and/or experiential background needed to integrate and apply the knowledge and skills delivered in the program. The B average minimum offers evidence that candidates are academically competent.

The CV and transcripts will allow the admissions committee to assess applicants' prior experience in the academic realm and, where applicable, the professional field. The applicants' Bachelor's degree will demonstrate the basic knowledge associated with the ability to achieve the proposed learning outcomes.

The statement of research interests will allow the admissions committee to assess applicants' ability to achieve learning outcome 10 as it relates to the ability to formulate complex and strategic forms of written and verbal expression. By assessing the relevance of the applicants' stated interests and experience to the program's holistic approach and offerings, the committee will better be able to gauge their likelihood of achieving all learning outcomes, in particular LO1 and LO2.

For applicants seeking the thesis option, meeting with the potential supervisor prior to admission can further add to this assessment. A list of supervisors with bios and identified research interests will be made available to applicants via a program website.

1.5.2 Alternative Requirements

There are no alternative requirements for this program.

1.6. Structure

1.6.1 Curriculum

The proposed MSc in Cybersecurity is an interdisciplinary program of study that will enhance the careers of

cybersecurity professionals by giving them a breadth of knowledge across both the business and technical aspects of cybersecurity.

There are two streams: **Cybersecurity Management** and **Cybersecurity Technology and Principles.** To achieve the intended holistic learning outcome, all students must take two core courses from their own stream and at least one core course from the other stream. The management core courses cover the fundamentals of risk management and governance and compliance; the technical core courses cover the fundamentals of security architecture and cybersecurity technology. Six elective courses, three from each stream, will be offered. The elective courses are designed to provide students with the tools to implement the principles outlined in the core courses.

Upon completion of this degree, students entering the program with a technical background will thus understand the business contexts of cybersecurity, and students from a management background will have knowledge of cybersecurity's technical aspects.

Courses

A) Cybersecurity Management

1. Cybersecurity Risk Management (Core course - M1)
2. Cybersecurity Framework, Governance and Compliance (Core course - M2)
3. Cybercriminology and Investigations
4. Security Operations, Business Continuity and Disaster Recovery
5. Privacy and Ethics

B) Cybersecurity Technology and Principles:

1. Fundamentals of Security Technologies (Core course – T1)
2. Security Architecture (Core course – T2)
3. Software Development Security
4. Network Security
5. Applied Cryptography

Pathways

The program will offer three different pathways to the MSc in Cybersecurity degree:

1. Master of Cybersecurity and Information Assurance (MCIA) (one year full-time)
   - **Course-based**: Students must take 8 courses, including the 4 core courses (one year full-time)
   - **Capstone**: Students must take 6 courses, including the 4 core courses, and complete a capstone project
2. **Master of Science with thesis**: Students must take 4 courses, including 3 core courses, and write a thesis (18 months–two years full-time).

Curriculum Structure

TABLE 5: Curriculum structure – course-based pathway

Year One					

Fall Term	Cr.	Winter term	Cr.	Spring/summer term	Cr.
Cybersecurity Frameworks, Governance, and Compliance	1	Cybersecurity Risk Management	1	Elective 3	1
Fundamentals of Security Technologies	1	Security Architecture	1	Elective 4	1
Elective 1	1	Elective 2	1		
SUBTOTAL	3		3		2

TABLE 6: Curriculum structure – capstone pathway

Year One					
Fall Term	**Cr.**	**Winter term**	**Cr.**	**Spring/summer term**	**Cr.**
Cybersecurity Frameworks, Governance, and Compliance	1	Cybersecurity Risk Management	1	Capstone	0
Fundamentals of Security Technologies	1	Security Architecture	1		
Elective 1	1	Elective 2	1		
SUBTOTAL	3		3		0

TABLE 7: Curriculum structure – thesis pathway

Year One					
Fall Term	**Cr.**	**Winter term**	**Cr.**	**Spring/summer term**	**Cr.**
Students choose two of the following three courses: Cybersecurity Frameworks, Governance, and Compliance Fundamentals of Security Technologies Elective 1 Thesis project development	2	Students choose two of the following three courses: Cybersecurity Risk Management Security Architecture Elective 2 Thesis project development, Continued	2	Thesis project development, Continued	
SUBTOTAL	2		2		

Year Two					

Fall Term	Cr.	Winter term	Cr.	Spring/summer term	
Thesis Project Development, continued		Thesis Project Completion		Potential extension	
SUBTOTAL					

Thesis Supervision

To be admitted to the thesis-based pathway, applicants must be matched to a supervisor or two co-supervisors. The applicants must mention in their letter of application the names of at least two professors who are affiliated with the program. The program will consult with the named professors. If there are more than one faculty interested in supervising a student, they can directly engage with the applicant about possible projects she/he can work on. The applicant can then decide on whom they want to work with. Once the applicant/supervisor agreement has been reached, the program will follow the process to admit the student. At the time of admission, the student has a supervisor who will help delineate the thesis topic and guide the student through the process of research and writing.

Oral Defence Committee

The thesis examination committee composition should follow the composition outlines in Procedure 21 of Policy 164. Committee membership is recommended to the GPD by the student's supervisory committee in consultation with the student. The examining committee will normally comprise the supervisor(s), two faculty members from the MSCIA program, and a non-voting chair, appointed by the program director.

1.6.2 GDLEs and Learning Outcomes

In order to meet the program's two overarching learning outcomes (LO1, LO2), the program is structured such that all students must take core courses from each of the two content streams: management and technology. Table 8 shows how each core course individually meets intended program learning outcomes, which themselves meet the master's level GDLES, as shown on Table 1 above. Elective courses, which provide deeper knowledge of the subjects covered in the core courses, further reinforce the program learning outcomes.

Each of the three pathways to the proposed MSCIA (please see 1.6.1) meets the intended learning outcomes and GDLES, with a slight variation in emphasis. The course-based pathway stresses the breadth and depth of knowledge of the field (GDLEs 1, 3); the capstone project pathway affords experience in an industry setting (GDLEs 3, 4); the thesis pathway stresses research and scholarship (GDLEs 2, 3, 6).

TABLE 8: Core Courses with Teaching and assessment methods mapped against program learning Outcomes

Core Course	Teaching	Assessment	Program Learning Outcomes
Cybersecurity Risk Management	Lecture, assigned readings,	Short assignments, case-analysis, group project, midterm, final exam	LO4, LO6

Cybersecurity Framework, Governance and Compliance	Lecture, assigned readings	Short assignments, case-analysis, group project, midterm, final exam	LO4, LO6
Fundamentals of Security Technologies	Lecture, assigned readings	Short assignments, labs, group project, midterm, final exam	LO5, LO6
Security Architecture	Lecture, assigned readings, lab	Short assignments, labs, group project, midterm, final exam	LO5, LO6

1.6.3 Program Length

As shown in Tables 5 to 7, the program will be structured so that students take three courses during each of the fall and winter terms, and two courses during the spring term for those in the course-based pathway. A course load of three credits per term will require commitment; assignments will be scheduled and structured to ensure that overall demands on students will be challenging but reasonable. Students in the capstone pathway will devote a term to that project, affording them time to work intensively with their industry partners to build on the knowledge they have acquired thus far and execute an industry-worthy project. Students in the thesis pathway will take three to four terms to complete their thesis, allowing them time to produce a document of quality, on the basis of which they will be well placed to apply to PhD programs.

1.7 Mode of Delivery

All courses will be taught in a lecture format with elements of discussion and experiential learning through exposure to technology and computer labs. Faculty will deliver the bulk of the lectures, with at least one invited guest speaker from industry per course. These speakers will each add a different perspective and communicate how businesses and nonprofits are dealing with recent developments in the key cybersecurity areas the courses cover.

In the technical stream, lecture material will be drawn not only from the faculty member's store of expertise, but also from textbooks (covering established and historic aspects of cybersecurity—LO3) and recent academic articles that analyze new developments (also LO3). Both will be used as launchpads for discussion.

In the managerial stream, textbooks will also be used to cover established and historic elements of information assurance, and industry documents setting out best practices and compliance requirements will be used to foster discussion about current real-world implications of the principles being taught (LO5).

In both streams, exams will assess students' comprehensive knowledge of the topics covered; lectures will be geared, and discussions steered, in large part towards enabling students to gain this knowledge. Mini-essays, as part of assignments and exams, will require them to communicate this knowledge effectively (LO6). Mid-term and/or finals exams could be skipped if students work on larger group projects covering independent study, research, as well as application and skill development.

Additionally, in the technical stream, students will undertake lab work that requires them to use software to complete a project modeled on real-life work (LO4, LO6). For example, they might be asked to design security architecture for a fictional product that will be implemented in an organization and have connections to the

cloud, making provisions for identity and access management. In the managerial stream, students will take on case studies asking them to analyze how cybersecurity works in certain real-life situations (LO3, LO5, LO6).

At the end of each course, students will undertake a larger group project involving all the key topics they have covered in class. By doing so, they will learn to work as part of a team and draw effectively on one another's complementary areas of expertise (LO1, LO2)—an essential skill in the field of cybersecurity, where solutions are developed by groups of people within an organization. They will also need to communicate effectively with one another and with instructors to complete their task (LO6).

Capstone projects will provide experiential learning that addresses holistic learning outcomes LO1 and LO2 as well as LO6 (communication) and other learning outcomes depending on the nature of the project.

The thesis project, similarly, will address LO1, LO2, and, through the writing and oral defence, LO6—as well as other learning outcomes depending on the thesis topic.

1.8 Resources

1.8.1 Human, Physical, and Financial Resources

Number of Faculty and Support Staff

The program will require 2 FTEs to be hired for teaching and supervision by the time the program launches with the aim to have 3rd hire shortly after the program launches. The delivery of the courses and supervision of students will also be supported by the six faculty members listed in section 1.8.2. In addition, one dedicated support staff member (1 FTE) will be required to oversee and administer the program.

Specialized Space Required

To deliver courses, the program will require one computer lab with a capacity of 35. Administrative space required will be one office for the program administrator as well as offices and common space for graduate students.

Preliminary Budget Information

The following table sets out the program requirements for which budgeting will be necessary.

TABLE 9: Preliminary budget information

Item	**Budget**
Number of courses	10 courses
Additional RFA faculty members	3 full-time
Graduate program staffing	1 full-time
Advertising and recruitment	$ to be costed
Additional space	TBD
Additional equipment	TBD
Guest speakers - honorariums	$ to be costed

Student Funding

Students are expected to apply for competitively adjudicated scholarships and awards—internally (e.g., the RGF) and externally (e.g., the OGS, OGF, and Canada Graduate Scholarships). These awards are listed below:

Ryerson Graduate Fellowship	up to $12,000
Ontario Graduate Scholarship (OGS)/Ryerson Graduate Scholarship (RGS)	$15,000
Ontario Graduate Fellowship (OGF)	$12,000
Canada Graduate Scholarships – Master's Program	$17,500

In addition to the above, the faculty can provide the students with stipends as well as provide opportunities to teaching assistantship.

Tuition

Tuition for the MSCIA will be based on the fees for Ryerson's Master of Science in Management, currently set at $10,121.78 for domestic students and $23,077.66 for international students. Students will pay tuition fees of 1/3 the annual amount per term, as per the university's policy.

1.8.2 Faculty

Proposed participating faculty for the MSCIA are drawn from TRSM-ITM, FOS-CS, and FEAS-ECBE. This list details faculty members' areas of teaching and research expertise.

Technical stream:

- Ali Miri is a full professor in the Department of Computer Science as well as the director of the Privacy and Big Data Institute and the director of the Information and Computer Security Laboratory. He has published extensively on security and privacy technologies and their applications, as well as cloud computing and big data. He has supervised over 70 students and overseen industry-related projects on security. He is a member of the Standards Council of Canada Big Data Working Group and the Ontario Centre of Excellence's College of Reviewers.
- Alex Ferworn is a full professor in the Department of Computer Science, where he is the graduate program director. He is also the graduate program director for the Master of Digital Media (YSGS). At the Chang School, he is the academic program co-coordinator of the Certificate Program in Data Analytics, Big Data and Predictive Analytics. He is also the academic coordinator of the Computer Security and Digital Forensics Certificate Program. His research focuses on computational public safety, particularly in the areas of urban disaster response and chemical, biological, radiological, nuclear explosive response.
- Muhammad Jaseemuddin is a full Professor and Program Director of Computer Networks in the Electrical, Computer & Biomedical Engineering. His areas of expertise include IP networks, Mobile Wireless Networks, Internet of Things, Mobile Computing, and Cloud Computing. He is leading Mobile Wireless Internet group in Wireless Networking and Communication Research (WINCORE) Lab at Ryerson University. His team has been working in the evolution of wireless access networks for multimedia services and multi-hop wireless networks including mesh and sensor networks. He is also involved in distributed and cloud computing with focus on edge cloud design for reliable and low-latency applications, and secure content caching.

Managerial stream:

- Atty Mashatan is an assistant professor at the School of Information Technology Management, director of the Cybersecurity Research Lab, and a member of the Privacy and Big Data Institute. Her research focuses on the development of novel cybersecurity designs based on emerging technologies

and is grounded in industry-relevant issues. She teaches courses on information systems security and privacy, cryptography and security, and enterprise architecture.

- Avner Levin is a full professor in the School of Business Management, where he teaches courses on legal issues in information technology and on governance and compliance in business. He has served as director of both the University Law Centre and the Privacy and Cyber Crime Institute and is a member of the Privacy and Big Data Institute and an affiliated faculty member of the Cybersecurity Research Lab. His research focuses on the legal regulation and protection of privacy and personal information in various sectors across jurisdictions, both within Canada and internationally, and he has published extensively on privacy and surveillance in the workplace and on social media.
- Bouchaib Bahli is a full professor in the Department of Information Technology Management, where he teaches courses on the analysis, design, and management of information systems. He is an affiliated faculty member of the Cybersecurity Research Lab. His research focuses on the strategic management of digital transformation, the automation of business services, risk management of IT projects, and outsourcing; he is often quoted by the media on these topics.

1.8.3 Program Type

This program will follow the standard model with the standard tuition and funded student slots. In other words, the program would receive some base funding support; the students would receive scholarship funding.

1.9 Executive Summary

The Master of Cybersecurity and Information Assurance is a proposed interdisciplinary graduate program arising from a collaboration between the Ted Rogers School of Information Technology Management (TRS-ITM) and the Department of Computer Science on the Faculty of Science (FOS-CS).

The program targets a societal need: the significant national and international shortage of trained cybersecurity workers. The professionals best suited to fill mid-to upper-level positions will be well-versed in both technical and managerial aspects of cybersecurity and will be able to address cyber risk with a holistic approach.

To produce such graduates, the MSCIA and MCIA programs will draw faculty members from both TRSITM and the Department of Computer Science to teach courses and supervise capstone projects and theses.

Students will participate in the program on a full-time basis at Ryerson's downtown campus, with the benefit of in-person instruction from recognized cybersecurity experts. The program will offer three pathways to a degree: a one-year course-based pathway, a one-year capstone pathway culminating in a project to be completed with an industry partner, and a two-year thesis pathway for those looking to pursue research in the field.

All participants will take four core courses—two each in the business and technical streams—and at least two electives. Upon graduation, they will be able to demonstrate thorough familiarity with the Common Bodies of Knowledge required for the globally recognized Certified Information Systems Security Professional (CISSP) program offered by $(ISC)^2$.

The program will enhance Ryerson's reputation as a leader in cybersecurity education and research. Its multidisciplinary training and research activity will complement the existing work of Rogers Cybersecure Catalyst and the Cybersecurity Research Lab.

The MSCIA will make Ryerson the first Canadian public research university to offer a multidisciplinary graduate cybersecurity program. As such, the university will further be able to support the Canadian government's pledge to make the country a leader in cybersecurity.

Moreover, as the first Ryerson collaboration between two faculties at the graduate level, the program will be poised to attract a range of students—including recent graduates and professionals alike—who wish to obtain a well-rounded graduate education in the field.

Administration

The program will be housed in the Yeates School of Graduate Studies. Its inaugural director will be Dr. Atefeh Mashatan, director of the Cybersecurity Research Lab and assistant professor of Information Technology Management. Faculty from TRS-ITM and FOS-CS will be involved in the development and implementation of the detailed curriculum.

Appendix I: Course Outlines -- Required Courses

COURSE NAME: Cybersecurity Risk Management

This is a required graduate course.

Calendar Description

This course gives an overview of internal and external cybersecurity risks to organizations and how they can be managed. It outlines the tactics, techniques, and procedures of threat actors, as well as their motivations and intent. It covers risk assessment, analysis, management, and treatment—as well as the frameworks, international standards, and guidelines that regulate these practices. It explains methods of equipping organizations to make informed business risk decisions, depending on their industries and the maturity level of their security programs.

Course Objectives

This course will introduce students to the key elements of cybersecurity risk management. It will provide students with the tools to understand the business impact on different industries of undesirable events or threat actors, as well as the tactics and motivations of threat actors. Students will be able to identify, assess, and analyze the probability and impact of cyber threats to an organization. They will be trained to suggest and apply appropriate strategies for managing risk.

Learning Outcomes

Upon completion of this course, students should be able to:

- Identify internal and external cybersecurity risks to an organization
- Understand the tactics and motivations of threat actors
- Demonstrate a thorough knowledge of regulatory frameworks, international standards, and guidelines that codify requirements and procedures for risk assessments, analyses, and management
- Understand different organizational risk assessment and risk treatment methods and evaluate their appropriateness
- Deploy qualitative and quantitative risk analysis methods to estimate the probability and the impact of cybersecurity incidents
- Assess impacts to organizations based on their security program's maturity level
- Develop and deploy tailored IT risk registers and risk-based cost-benefit analysis to support management decision-making

Required Reading - TBD

Methods of Assessment - Assignments, labs, projects: 20%
Group project: 25%
Midterm examination: 25%
Final examination: 30%

COURSE NAME: Cybersecurity Frameworks, Governance, and Compliance

This is a required graduate course.

Calendar Description

This course gives an overview of the regulatory and industry-driven frameworks that govern an organization's cybersecurity program. Topics covered include the governance, risk, and compliance (GRC) concepts that apply to cybersecurity; the role of a Chief Information Security Officer (CISO), including its historical evolution; the implementation of cybersecurity governance within a business risk program; and methods of achieving cybersecurity compliance within an IT risk management program.

Course Objectives

This course will introduce students to the key aspects of cybersecurity management beyond risk management itself. Students will learn how to assess an organization's security program by using GRC (governance, risk, and compliance) concepts and their associated frameworks. The course will outline the evolving duties and purview of Chief Information Officers (CISOs). Students will be equipped to recommend IT risk management solutions to organizations, and to implement them.

Learning Outcomes

Upon completion of this course, students should be able to:

- Identify and understand the various frameworks governing an organization's IT risk management program
- Be able to communicate effectively with upper management and auditors about these frameworks
- Analyze the importance of a Chief Information Security Officer to an organization
- Evaluate an organization's implementation of cybersecurity governance within its larger business risk program
- Use managerial, procedural, and technical controls to manage risks
- Understand cybersecurity compliance and how it fits into an organization's IT risk management program
- Evaluate an organization's compliance with industry and regional cybersecurity regulations
- Conduct an IT audit
- Deploy attestation to assess controls in an organization's IT risk management program
- Develop a compliance risk register
- Be prepared to implement an IT risk management program

Required Reading - TBD

Methods of Assessment - Assignments, labs, projects: 20%
Group project: 25%
Midterm examination: 25%
Final examination: 30%

COURSE NAME: Security Architecture
This is a required graduate course.

Calendar Description

This course will explore the concept of security architecture in a time of change. Where traditional security architectures involved protecting the "perimeter" of the organization's network, many organizations are moving to cloud-hosted services. The course will cover the security architect's role in assessing what information can and should be stored in the cloud, and in setting up security infrastructure—as it applies to IT networks, data protection, security monitoring, and auditing.

Course Objectives

This course will explain the principles of security architecture and introduce students to its evolution. Students will learn the benefits and risks of moving information to the cloud and how security measures can enable an organization to achieve regulatory compliance and reduce liability. The course will cover agreements with cloud providers and teach students to develop cloud security architecture.

Learning Outcomes

Upon completion of this course, students should be able to:

- Explain the information security principles underlying an organization's architecture system
- Understand traditional security architecture and evaluate the protection of an organization's network perimeter
- Track the evolution of security architecture as organizations move more information to the cloud
- Evaluate the challenges and risks involved in trusting information to a cloud provider
- Be able to strategically align an organization's information security goals with the solutions the organization is designing
- Use appropriate frameworks to evaluate an organization's existing security architecture
- Understand how different jurisdictions affect what information can be stored in the cloud
- Decide how much of an organization's information should be stored in the cloud, taking into account liability
- Evaluate agreements with cloud providers on the basis of compliance and audit considerations
- Develop logical security architecture to help an organization achieve its information security and privacy goals

Required Reading - TBD

Methods of Assessment - Assignments, labs, projects: 20%
Group project: 25%
Midterm examination: 25%
Final examination: 30%

COURSE NAME: Fundamentals of Security Technologies

This is a required graduate course.

Calendar Description

This course provides an overview of the technology that is fundamental to an organization's cybersecurity program and considers how it can best be deployed. It focuses on the principles of identity security and access management (IAM) as well as the protection of data, the world's modern currency. Concepts covered include role-based access, access modeling, trust models for access control, privileged account management, credential management, and authentication. The course will also discuss the way innovation works in cybersecurity.

Course Objectives

In teaching the principles of security engineering and how to apply them, this course will introduce students to the duties and tools of the security engineer. It will enable students to assess and bolster an organization's identity and access management (IAM) and to protect its data. Students will learn the importance of innovation in cybersecurity and how it can be integrated with existing technology. Each will develop an idea for an innovative technology or process.

Learning Outcomes

Upon completion of this course, students should be able to:

- Understand and apply the principles of identity and access management with respect to infrastructure, platforms, and application access controls
- Understand and implement trust models for access control
- Explain the workings of Public Key Infrastructure (PKI) for certificate management and federated identity
- Apply the principles of governance risk and compliance to an organization's credential management
- Explain and apply the principles of configuration management
- Track all of the assets in an organization's environment
- Understand the role of vulnerability management within overall IT risk management
- Identify, appropriately handle, and secure critical data within an organization
- Differentiate between protection and access control approaches to data
- Design and develop data classification guidelines for an organization's data security program
- Analyze the importance of innovation in cybersecurity and how it may best be implemented
- Develop an idea for an innovative technology or process

Required Reading - TBD

Methods of Assessment - Assignments, labs, projects: 20%
Group project: 25%
Midterm examination: 25%
Final examination: 30%

Appendix II: Development Schedule

The anticipated launch of the program is the 2023–2024 academic year. Working back from the launch date, the tentative timeline for development of the program is as follows.

Development Stages	**Time Period**
Develop a draft LOI	December 2019–April 2020
Draft LOI shared with the YSGS working group for feedback	May 2020
Finalize the LOI, including consultation with the curriculum development consultants on the learning outcomes	June 2020
YSGS submits the LOI to the University Planning Office for financial review	July 2020
LOI posted for 30 days (Following the UPO approval, the LOI is publicly posted for 30 days by the Provost's Office)	January 2021
Authorization to proceed (The Provost issues a letter of authorization to proceed to the development of the full proposal)	February 2021
Full proposal development	March 2021 – June 2021
Draft proposal shared with the YSGS working group for feedback	July 2021
Full proposal reviewed by the Planning and Programs committee of YSGS Council	August 2021
Approval processes to commence (per Policy 112)	September 2021
Invite peer review team and schedule visit	October 2021
Peer review team visit	November/December 2021
Peer review team report	January 2021
Response by program	March 2022
Senate	May 2022
Quality Council	June 2022
Submission to Ministry	August 2022
Advertisement for the new program	Fall 2022–ongoing
Launch	Fall 2023

TED ROGERS SCHOOL OF MANAGEMENT

Office of the Dean

January 14, 2021

RE: Letter of Support for the MSCIA and the MCIA Programs

To whom it may concern:

I write this letter with great enthusiasm in support of the Master of Science in Cybersecurity and Information Assurance (MSCIA) and the Master of Cybersecurity and Information Assurance (MCIA) programs. These interdisciplinary programs are sure to contribute significantly to the portfolio of our university's graduate programs as information security and its management are among the top concerns for enterprises of all kinds and sizes. In addition, they have significant impact on individuals and society as a whole.

As indicated in the proposal these programs offer "a multidisciplinary learning experience, providing students with an integrated framework for dealing with cyber threats, risks, and vulnerabilities from both technical and business perspectives." Such a learning experience is invaluable to a variety of students as the subsequent skills are critical. In addition to what is already mentioned in the LOT, these new programs will nicely complement our existing MBA program, which is our flagship professional program that aims to produce business professionals with a broad view of all aspects of business and management where the management of information and its security are critical aspects. Our other professional program in health services management can equally benefit from the skill set and body of knowledge these new programs offer as the security and privacy of health information is of upmost importance. Cybersecurity is also a fundamental block of our digital enterprise area in which we have a PhD specialization, which would be an attractive target for some graduates of these proposed programs.

From a strategic point of view, we agree with the value proposition of this program as indicated in the LOI and believe that the supply in the market is still well behind the demand. The programs will be supported by a unique group of outstanding faculty from TRSM who are experts on the technical, managerial and legal aspects of information security therefore we have full confidence that the program will be adequately supported.

In conclusion, we believe our university's move into the cybersecurity space in graduate education is more than timely, and it reflects our strengths and the needs of our stakeholders. We believe the proposed programs are well positioned and feasible. TRSM has the potential and willingness to support the faculty sourcing of these programs.

Sincerely,

Daphne Taras
Professor & Dean
Ted Rogers School of Management
Ryerson University

Ryerson University
Faculty of Engineering & Architectural Science

January 17, 2021

Professor Cory Searcy
Vice-Provost and Dean, Yates School of Graduate Studies

RE: Letter of Support for the MSCIA and the MCIA Interdisciplinary Programs

Dear Professor Searcy,

It is my pleasure to convey my strong support for the proposed interdisciplinary Master of Science in Cybersecurity and Information Assurance (MSCIA) and the Master of Cybersecurity and Information Assurance (MCIA) programs. From the LOI it is clear that these programs are addressing a very important and broad societal need. It is also clear that there is a very strong market-demand for graduates from such a program.

The interdisciplinary approach combining both the technical and managerial aspects of cyber security provides for a comprehensive approach and will make this a very attractive program for students interested in this area. FEAS is pleased to participate in this effort which complements our MASc/MEng programs in Computer Networks and our ongoing research efforts in the area of Cyber Security like the appointment recently of Professor Arani of the Department of Electrical, Computer and Biomedical Engineering to a Tier 2 CRC in Smart Grid Cyber-Physical Security.

The program clearly fits into Ryerson University's Strategic Research Plan which lists cybersecurity as an "immediate global issue" and lists it as an area of focus. The program will produce graduates with a new set of skills with which they can address these issues. As mentioned in the LOI the program also addresses the areas of "City Building" and "Inclusion" mentioned in both the Strategic Research Plan and Academic Plan.

In summary this program is addressing an urgent and timely societal need and builds on the strengths present at Ryerson University enabling us to become a leader in this area. FEAS is well positioned to contribute to this initiative.

Best regards,

Tom Duever, PEng
Dean, Faculty of Engineering and Architectural Science
Ryerson University

350 Victoria Street
Office: ENG 374
Toronto, ON, Canada M5B 2K3

t: 416.979.5140
f: 416.979.5233
tom.duever@ryerson.ca

ryerson.ca/feas

Ryerson University

Faculty of Science

Professor Cory Searcy
Vice-Provost and Dean, Yates School of Graduate Studies
RE: Letter of Support for the MSCIA and the MCIA Interdisciplinary Programs

Dear Professor Searcy,

I would like to provide my strong support for the proposed interdisciplinary Master of Science in Cybersecurity and Information Assurance (MSCIA) and the Master of Cybersecurity and Information Assurance (MCIA) programs. From the LOI that I received, it is clear that these programs address a critical problem and demonstrate broad societal need. One only needs to peruse the newspaper headlines to understand the urgency of the need. It is also clear that there is a very strong market-demand for graduates from such a program.

The proposed interdisciplinary approach combines both the technical and managerial aspects of Cybersecurity, thus providing a comprehensive approach that will make this a popular program for students interested in this discipline. The technical methods in Cybersecurity can be considered a subfield of Computer Science since students require a deep understanding of computers and networks to understand and prevent data breaches and attacks, monitor systems, and create software and hardware solutions to mitigate these. The FOS houses the Departments of Computer Science and Mathematics, where our professors have ongoing Cybersecurity research efforts. Examples include, amongst others, from Computer Science Drs. Alex Ferworn (Computational Public Safety), Ali Miri (Cybersecurity and Computer Networks), Drs. Jelena and Vojislav Misic (Security and Internet of Things (IoT)) and Dr. Jake Doliskani (Cryptography and Quantum Computing) and from Mathematics Dr. Peter Danziger (Cryptography) and Dr. Chul Kim (Cryptography, Cryptanalysis and Network Security). Future hires are also anticipated in this discipline, particularly considering the new Cyber Studies Minor and the plan to create a Cyber Studies major.

The program fits into Ryerson University's Strategic Research Plan, which lists Cybersecurity as an "immediate global issue" and an area of focus. The program will produce graduates with a set of skills to address the issues mentioned above. The program also addresses the areas of "City Building" and "Inclusion" mentioned in the Strategic Research Plan and Academic Plan.

In summary, this program addresses an urgent and timely societal need. It builds on the strengths present at Ryerson University and the Faculty of Science, enabling us to become a leader in this area. The FOS is ideally positioned to contribute to this initiative.

Sincerely,

Dean, Faculty of Science

350 Victoria Street
Toronto, ON, Canada M5B 2K3
t: 416-979-5251