

CYBERSECURITY LEADERSHIP AND CYBERPRENEURSHIP

The Master of Cybersecurity Leadership and Cyberpreneurship (MCLC) program is focused on training working professionals to become ethically minded leaders in cybersecurity and future chief information security officers (CISOs) in organizations ranging from start-ups to established multinational companies. The MCLC students benefit from rich experiential learning opportunities throughout the program's curriculum. This program integrates ethical considerations of cybersecurity in various domains to deliver graduates with unique skills and dispositions that will fill the pressing societal need for cybersecurity leaders.

Administrative Staff

Director and Graduate Program Coordinator

Ali Dehghantanha (150 Research Lane Suite 120C)
graddir@socs.uoguelph.ca

In-program Graduate Program Specialist

cyberadmin@uoguelph.ca

Graduate Admissions Specialist

cyberapps@uoguelph.ca (cybersapps@uoguelph.ca)

Graduate Faculty

This list may include Regular Graduate Faculty, Associated Graduate Faculty and/or Graduate Faculty from other universities.

Ruben Burga

B.A.Sc. Toronto, MBA Bryant, PhD Guelph - Assistant Professor
Graduate Faculty

Rozita Dara

B.Sc. Shahid Teheshti, M.Sc. Guelph, PhD Waterloo - Associate Professor

Graduate Faculty

Ali Dehghantanha

BSE Azad, M.Sc., PhD Putra Malaysia - Professor
Graduate Faculty

Jamie Gruman

BA Concordia, MA Lakehead, PhD Windsor - Professor
Graduate Faculty

Andrew Hamilton-Wright

B.Sc., M.Sc. Guelph, PhD Waterloo - Associate Professor
Graduate Faculty

Louise Hayes

B.Sc., MBA British Columbia, PhD Waterloo, CPA, CA - Associate Professor
Graduate Faculty

Hassan Khan

B.Sc. NUST, M.Sc. Southern California, PhD Waterloo - Associate Professor
Graduate Faculty

Xiaodong Lin

B.A.Sc. Nanjing, M.Sc. East China Normal, PhD Beijing, PhD Waterloo - Professor

Graduate Faculty

Charlie F. Obimbo

M.Sc. Kiev, PhD New Brunswick - Professor
Graduate Faculty

Davar Rezanian

M.Sc. Utrecht, MBA Derby, PhD Ramon Llull, CPA, CMA - Associate Professor
Graduate Faculty

Admission Requirements

To be considered for admission, applicants must:

1. Be qualified graduates a four-year honour's undergraduate degree from a recognized university, typically in Computer Science, Information Systems, Business, Management, or an equivalent program (minimum Baverage); and
2. Have a minimum of three years of relevant work experience, as determined by the admissions committee.

Applicants should clearly demonstrate the relevance of their work experience in the statement of intent and resume submitted with their application. Applicants with more than five years of work experience will be given preference by the admissions committee.

Additionally, all applicants must meet the University of Guelph's English Language Proficiency requirements for admission. If an applicant's first language is not English, or their undergraduate degree was not taught at an English-language institution, an English Language Proficiency test will be required. Applications from qualified members of under-represented groups are encouraged.

Learning Outcomes

Upon successful completion of the Master of Cybersecurity Leadership and Cyberpreneurship, graduates will have the capacity to practice the following:

1. **Security Management and Governance:** The practice and design of security governance, program development and management, incident management and risk management along with abilities to assess, design, implement and manage IT governance and business systems. Graduates will be able to:
 - a. Design and implement enterprise security governance programs.
 - b. Design, implement and assess enterprise incident and risk management programs.
 - c. Assess, design, implement and manage IT governance systems in alignment with business requirements.
2. **Security Audit and Information Systems Control:** The ability to audit, control, monitor and assess an organization's IT and business systems, identify associated risks, and implement controls to manage those risks. Graduates will be able to:
 - a. Identify and manage enterprise IT risk.
 - b. Implement and maintain risk registers and risk controls.
 - c. Implement privacy by design to IT systems, networks and applications.
 - d. Develop controls: defence controls, offensive controls, investigative controls (digital forensics).
3. **Project Management and Governance:** The ability to plan, resource, schedule and control project processes and deliverables, make use of financial information and manage teams to deliver cybersecurity solutions on time and on budget. Graduates will be able to:

- a. Apply Project Management tools in planning, executing, controlling, and closing a project through its lifecycle.
 - b. Input and analyze key financial information and its implications in consultation with financial managers to affect strategy, operations, and performance.
 - c. Create project management documents related to project scope, plan, schedule, risk, communication, quality and project closing.
 - d. Optimize a project while managing the triple constraints of time, cost, and scope.
 - e. Report project progress effectively to project stakeholders in oral and written format.
 - f. Use negotiation skills in initiating and managing changes to project scope.
 - g. Identify and analyse the ethical considerations implicit in managing projects, including the potential effects on project owner, sponsor, and users.
4. **Cyberpreneurship and Organizational Change Leadership:** The ability to lead organizational change and manage innovation and entrepreneurship within organizations and teams. Graduates will be able to:
- a. Assess technological solutions with respect to their technical, market and financial feasibility.
 - b. Develop business models and manage projects under high uncertainty.
 - c. Understand and utilize key skills related to entrepreneurship, relationship building, organizational change, as well as project and personnel management.
 - d. Develop a strategy to lead a change effort within an organization.
 - e. Design a process for promoting change in an organization.
 - f. Implement skills related to change management (e.g., communication).
 - g. Identify potential weak points that could undermine a change effort, and address sources of resistance to change.
 - h. Critically analyze new information regarding change that you may encounter.
 - i. Understand the process and the analytical tools that can assist in the innovation and commercialization process and how best to prepare technologies to survive commercialization.
5. **Professional Capacity:** Professional Capacity entails the ability to abide by ethical guidelines, laws and regulations. It involves the ability of the graduate to work collaboratively and independently in regional and global contexts. Graduates will be able to:
- a. Demonstrate ethical behaviour consistent with academic integrity and the professional code of ethics as required in cybersecurity and threat intelligence.
 - b. Collaborate on and conduct in-depth research about different cyber threats and prepare relevant technical and non-technical reports.
 - c. Exercise entrustable professional skills including initiative, responsibility, accountability and decision making in complex situations.

Code	Title	Credits
CIS*6790	Executive Seminar in Cybersecurity ¹	0.25
CIS*6710	Principles and Practices of Information Security	0.50
CIS*6720	Cybersecurity Management and Governance	0.50
BUS*6180	Financial and Managerial Accounting	0.50
BUS*6190	Cyberpreneurship	0.50
LEAD*6200	Leadership of Organizational Change	0.50
MGMT*6400 or CIS*6730	Project Management Cybersecurity Management and Governance Project	0.50

¹ MCLC students must complete CIS*6790 twice.

Students who seek approval from the Program Director may opt to take 4.00 graduate credits inclusive of a major research project (CIS*6730 Cybersecurity Management and Governance Project). If students are approved to complete the major research project, then it will be in lieu of MGMT*6400 Project Management.

Program Requirements

The program requires successful completion of 3.5 graduate credits as follows: