

CYBERSECURITY STUDIES MINOR

For Bachelor of Arts and Bachelor of Science

The Cybersecurity Studies Minor is an interdisciplinary program with coursework from three Faculties/Schools – The Faculty of Arts and Science (Department of Computer Science), the Faculty of Health and Community Studies (Department of Public Safety and Justice Studies), and the School of Business (Departments of Accounting and Finance, and Management and Organizations). The minor requires coursework in information security, cyber threat and risk assessment, cybersecurity and digital investigations, and introductory business and financial accounting. Integrating business courses into the cybersecurity studies program ensures that students are equipped to understand and address the broader business context in which cybersecurity operates. This is essential for effectively managing cyber risks and protecting an organization's interests.

The Cybersecurity Studies Minor is 18 senior-level credits. Students must complete the junior-level prerequisite course CMPT 101 or equivalent.

Code	Title	Credits
Minor Requirements		
ACCT 311	Introductory Accounting	3
BUSN 201	Introduction to Sustainable Business	3
CYCS 200	Information Security, An Overview ¹	3
CYCS 300	Introduction To Cyber Risk Management	3
CYJU 265	Cybersecurity and Digital Investigations	3
CYJU 365	Navigating the Future of Cybersecurity Investigations	3
Total Credits		18

1

Students who take CMPT 280 (Introduction to Cybersecurity) cannot take CYCS 200. Instead, these students can choose from ACCT 315, ACCT 442, CMPT 310, CYJU 223, ORGA 312, or SOCI 225 to complete the minor requirements.

Program Learning Outcomes

1. Explain how cybersecurity issues intersect with the justice system, including knowledge of cybercrime laws, regulations, and the legal procedures involved in prosecuting cybercriminals.
2. Identify ethical dilemmas, consider various perspectives, and make decisions that prioritize justice, privacy, and digital security.
3. Demonstrate an understanding of cyber threats and best practices for online safety, as well as tools and techniques for protecting personal and professional data.
4. Conduct a cyber risk assessment and communicate actionable choices, including benefits and limitations, to executive decision-makers.
5. Demonstrate a solid understanding of fundamental business concepts and functions, including business planning, management, ethics, entrepreneurship, and sustainability, providing a broader context for cybersecurity operations within business environments.