

Déployer l'Institut multidisciplinaire en cybersécurité et cyberrésilience



Se mobiliser pour une société cyberrésiliente et innovante

L'Université de Montréal, Polytechnique Montréal et HEC Montréal unissent leurs forces – et le pouvoir d'action de leurs amis et amies philanthropes – pour aider la société à faire face à l'un des plus grands enjeux de notre époque : la cybersécurité.

Pourquoi agir maintenant

Les technologies de l'information et de la communication, l'intelligence artificielle et le déploiement massif d'objets connectés transforment fondamentalement nos sociétés, y apportant des avantages considérables. Mais de nombreux événements nous rappellent quotidiennement que ces avancées ouvrent également la voie aux cybermenaces, ce qui fragilise énormément nos systèmes économiques et démocratiques, de même que la sécurité, la situation financière et la santé même des personnes qui en sont victimes.

Développer une meilleure capacité d'impact

Ces enjeux complexes demandent la mise en commun de forces académiques multidisciplinaires et un mécanisme de collaboration authentique. Les expertises, technologies, connaissances de pointes développées et transmises au sein des institutions universitaires doivent pouvoir s'intégrer avec efficacité au sein de l'écosystème industriel et gouvernemental de la cybersécurité.

L'Institut multidisciplinaire en cybersécurité et cyberrésilience (IMC²) propose une façon novatrice d'aborder la cybersécurité, qui englobe les aspects humains, technologiques et de gestion. Son approche est sans équivalent au Québec.



Nos forces combinées

En unissant nos expertises, nous créons et offrons des solutions à tous les niveaux : technologique, réglementaire et politique, de même qu'en formation et en management.

L'IMC², en bref

Les enjeux sociétaux liés à la cybersécurité demandent que le monde universitaire déploie une capacité d'impact et d'influence allant au-delà de ce qui est fait aujourd'hui.

Notre Institut interuniversitaire va donc plus loin que la recherche et l'enseignement en plaçant les citoyennes et citoyens au cœur de ses préoccupations et en mobilisant ses forces vives pour que les fruits de ses travaux débouchent sur des innovations concrètes et ancrées dans la réalité du terrain.

L'IMC² va également au-delà des approches universitaires traditionnelles en cybersécurité en mettant de l'avant la prévention, l'adaptation continue et la collaboration afin de développer une approche axée sur la cyberrésilience.

Ce que nous allons faire

En fédérant l'ensemble de nos ressources, nous pourrons réaliser des projets multifacultaires ambitieux, innovants et transformateurs qui toucheront :

1. La formation

Préparer la relève aux grands défis sociétaux en cybersécurité

2. La recherche et l'innovation

Développer des réponses aux grands défis sociétaux en cybersécurité

3. Les politiques publiques

Contribuer au développement d'une société cyberconsciente et cyberresponsable

*Notre vision : une société cyber résiliente
innovante grâce à la mobilisation de
forces vives multidisciplinaires*

Les investissements requis

Un investissement de plus de 44,55 M\$ est requis pour soutenir pendant 5 ans les trois volets d'un institut sans équivalent au Québec.

Les coûts mondiaux de la cybercriminalité sont en constante augmentation. À eux seuls, les rançongiciels coûtent à leurs victimes des milliards de dollars chaque année, impactant ainsi les fondements socio-économiques de nos sociétés. En parallèle, la pénurie de main-d'œuvre en cybersécurité est une préoccupation majeure, mettant en péril notre capacité à faire face aux cybermenaces en constante évolution.

Ces facteurs mettent en lumière le besoin de collaboration dans l'écosystème, au sein duquel le monde académique doit jouer un rôle central. Les forces vives de l'IMC² – avec ses 44 chercheurs et chercheuses ainsi que leurs équipes – travaillent déjà à trouver des solutions, en synergie avec les acteurs clés de la cybersécurité à Montréal et au Québec.



Marc Gervais,
directeur exécutif de l'IMC²



Impacts transformateurs

1. Impacts pour la communauté étudiante

- Accès à une offre de formation de haut calibre favorisant la mobilisation de compétences.
- Possibilité de s'intégrer à un nouveau groupe de recherche multidisciplinaire.
- Soutien aux initiatives entrepreneuriales liées à la cybersécurité et à la cyberrésilience.

2. Impacts pour les individus

- Meilleure conscientisation face aux enjeux en cybersécurité.
- Capacité à mieux déceler les tentatives d'hameçonnage et de cyberfraude.
- Soutien en cas d'incident.

3. Impacts pour l'économie

- Amélioration de la cybersécurité des entreprises et institutions québécoises, y compris les plus vulnérables (municipalités, hôpitaux, écoles, PME & OSBL, communautés autochtones) via une offre de services de sensibilisation, de formation, de recherche et d'innovation adaptés à leurs besoins.
- Offre d'une main d'œuvre hautement qualifiée et sensibilisée aux aspects technologiques, humains et de gestion de la cybersécurité.
- Amélioration de la protection et de la résilience des infrastructures critiques.

Contacts

Université de Montréal

MICHAEL PECHO

Vice-recteur à la philanthropie et à l'engagement des diplômés,
UdeM philanthropie et diplômés

C : 514 793-7499

michael.pecho@umontreal.ca

ALEXANDRA JEANTY, MBA

Directrice des dons exceptionnels, UdeM philanthropie et diplômés

C : 514 919-0680

alexandra.jeanty@umontreal.ca

Polytechnique Montréal

VALÉRIE BELISLE

Directrice Philanthropie et Relations avec la communauté diplômée

T : 514 340-3246

valerie.belisle@polymtl.ca

Fondation HEC Montréal

MICHEL PATRY, Ph.D.

Président-directeur général, Fondation HEC Montréal

T : 514 340-6458

michel.patry@hec.ca

MÉLANIE GAGNON

Directrice, Direction de la Fondation HEC Montréal
et des relations avec les diplômés

T : 514 340-6079

melanie.gagnon@hec.ca