ACADEMIC COUNCIL REPORT

SESSION:

Public ☒

ACTION REQUESTED:

Decision ☒
Discussion/Direction ☐
Information ☐

Financial Impact ☐ Yes ☒ No **Included in Budget** ☐ Yes ☒ No

TO: Academic Council

DATE: April 28, 2020

PRESENTED BY: Les Jacobs, Vice-President, Research and Innovation

SUBJECT: Establishment of the Institute for Cyber Security and Resilient Systems (ICSRS) at Ontario Tech University

COMMITTEE/BOARD MANDATE:

Recommendation:

The Research Board, at its April 24, 2020 meeting, reviewed the proposal by Dr. Khalil El-Khatib from the Faculty of Business and Information Technology to establish the Institute for Cyber Security and Resilient Systems (ICSRS) and unanimously approved the motion of a recommendation that it goes forward to Academic Council.

We request that Academic Council review the proposal for the Institute and find it appropriate to recommend to the Board of Governors for approval.

BACKGROUND/CONTEXT & RATIONALE:

There has been a sharp increase in the number of cyberattacks over the last few years, costing businesses trillions of dollars, in addition to the loss of billions of personal and financial records (and possible meddling with elections) [1]. In addition, recent advancement in computation and communication, coupled with the proliferation of the Internet and the rush to replace physical systems with more digitally enabled systems have made cybersecurity an international challenge. What is even more important is that the threat landscape has changed

1. TrendMicro - Unseen Threats, Imminent Losses - 2018 Midyear Security Roundup. Available at https://documents.trendmicro.com/assets/rpt/rpt-2018-Midyear-Security-Roundup-unseen-threats-imminent-losses.pdf. Accessed on Oct 17, 2018.

over the last few years, with an increase in state-sponsored attacks, which clearly shows that governments around the world have been investing in cybersecurity capabilities.

While the majority of public and private organizations currently use various solutions to protect themselves from potential cyberattacks, there is rarely a day that we do not hear news about cyber security incidents. Whether it is ransomware, distributed denial of service (DDOS), phishing or spear phishing, drive-by, password SQL injection, eavesdropping, social engineering or any other form of attack, these attacks are inflecting havoc on various sectors of the Canadian economy (more than $3 billion in economic losses each year [2]). Some of these attacks also inflicted damages on the lives of millions of Canadians. In November 2019, threat actors managed to infect all Nunavut government electronic services with a ransomware that paralyzed all operations. A number of Ontario municipalities (Stratford, Woodstock and The Nation) were also hit with ransomware attacks. Ransomware hit three Ontario hospitals crippling their computer system and locking access to patients' medical data. In August 2019, the Five Eyes alliance that includes Canada, the United States, New Zealand, Australia, and the UK, accused China of running a 12-year campaign of cyber espionage to steal trade secrets and intellectual properties from companies in 12 countries around the world. In December, security researchers from Palo Alto Networks attributed a campaign to infect various government agencies in four continents with malware to the Russian cyber-espionage group Sofacy. Last but not least, a cyberattack recently targeted a major Czech hospital during the current COVID-19 pandemic forcing the hospital to shut down its whole IT infrastructure, and the emails and passwords of personnel from the World Health Organization (WHO), the Centers for Disease Control and Prevention (CDC) and other health organizations were posted online.

Cyberspace is a unique environment where IT, business and people intertwined together, making it a challenge to systematically enforce procedures and maintain security. It is common knowledge in cybersecurity that the single weakest link in the information security chain is always the human being, and that most of the cybersecurity incidents are the results of human actions (or inactions). Therefore, in order to improve security in cyberspace, it is important to factor the human aspect of any security solution. Ensuring a secure and robust cyberspace requires a solid understanding of human nature and its role in the whole cyberspace ecosystem; factors such as the acceptability of cyber policies and controls, understanding the motivations behind cyberattacks, the background of cyber victims and criminals, and identifying and eliminating insider threats are all challenges rooted in social and behavioral science.

The traditional view of cybersecurity in a binary form (secure vs. insecure, verified vs. unverified etc.) is also changing rapidly. An emerging paradigm focuses on the concept of *trust* as the basic description of an entity's reliability, performance and security. A trust-based cyberspace can be described as an infrastructure for information exchange in which the accuracy, integrity and confidentiality of information are not deterministic and binary, but instead are based on a dynamic trust score. Such trust scores can be assigned to multiple different network entities, which can be are based on multitude of factors based on reputation, reliability, performance and past history. Such trust scores are both subjective and dynamic: an action, lack of action or state change could alter, and even potentially rescind the trustworthiness of an entity inside or outside the cyberspace. This new paradigm will form the basis for a *resilient* cyberspace, in which every entity (physical, logical, or information) is evaluated dynamically and constantly based on the events in the cyberspace, and actions/decisions are taken to maintain or improve the cyber resilience in face of those events.

---

[2]. National Cyber Security Action Plan (2019-2024) Available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx

Along with resilience, the issue of privacy has also become one of the most important topics of discussion today. For a majority of consumers, getting better services in a digital economy may be worth sacrificing the confidentiality of some private data by making it available to service providers or to the public, as long as they can trust the ability of the service provider to keep it safe. However, there are few alternatives for those who may prefer to have a choice in this matter and control what information they provide to the companies. The current deployment of technology does not provide many choices to such customers. Whether people want or not, their utility usage, internet access, cell phone location and vehicle information is collected and maintained individually by service providers, making an anonymous life impossible. As more advanced technologies for smart cities are developed, maintaining such anonymity becomes harder.

Today, a large, yet fragmented, number of research activities related to cyber security is done by a number of researchers and in different research labs, with a large concentration of security, privacy and trust happening within the Faculty of Business and Information Technology, with a fairly large number of social science research happening with the Faculty of Social Science and Humanities (FSSH), in addition to some research on software security happening within the Faculty of Engineering and Applied Science (FEAS), and nuclear physical security happening in the Faculty of Energy and Nuclear Science (FENS). Though Ontario Tech University is a small university, most of the research still happens in silos. The main objective of the proposed institute is to create a fertile ground for potential collaboration between researchers from different disciplines to address cyber security and resilience challenges. More specifically, the Institute will allow researchers to:

- Create opportunities for researchers from multiple disciplines to network, collaborate and share ideas.
- Address bigger challenges in cybersecurity and resiliency and make larger and impactful solutions to society.
- Allow faculty members from faculties that do not have graduate programs to participate in student supervision.
- Leverage the power of an institute when applying for individual or large grants (Canada Foundation for Innovation, NSERC Collaborative Research and Training Experience Program (CREATE), NSERC Networks of Centres of Excellence (NCE), New Frontiers in Research Fund, SSHRC Partnership grants.

RESEARCH MANDATE

One of the institutional priorities for Ontario Tech is “Tech with a conscience” which is defined as the responsible and ethical use and development of technologies that can help with the progress and prosperity of humanity. As today’s technology is intertwined with the daily artifacts and applications spanning multiple domains, it is imperative to tackle the human-business-technology challenge from an interdisciplinary perspective. Being at the front of research and use of technology, and with a large concentration of faculty members carrying leading-edge research in Information Technology (Security, Privacy, Trust) and Social Science (business, law and ethics), Ontario Tech is strategically situated for developing and evaluating the impact of new technologies on our society. Being a small and innovative university, and with many cross-appointments and collaborations between many faculty members, establishing a research institute will provide the rich environment to cultivate and promote research on the influence of new security, privacy and trust technologies on human and society, as well as guiding the design and development of future technologies.

The Faculty of Business and Information Technology has taken a major initiative to develop a cybersecurity research institute, called the Institute for Cyber Security and Resilient Systems (ICSRS), with a mandate to research the intersection of technical, legal, social, economic and

ethical implications of privacy, security and trust technologies. The Institute will create a focal point within Ontario Tech University, for research, teaching, and outreach in the field of cyber security protection (e.g. critical infrastructure protection, identity management, protection from social engineering, secure software system, password protection, …) to enhance online and offline cyber protection and innovation. The focus of the Institute will be broadly to examine issues surrounding the use and protection of emerging technologies in both public and private sectors. The Institute links to three of Ontario Tech strategic research priorities from the newly released strategic research DRIVING THE FUTURE THROUGH, RESEARCH EXCELLENCE STRATEGIC RESEARCH PLAN, 2020-2025.

The Institute would address the following Ontario Tech priorities:

- Attract and retain outstanding national and international academics
- Place priorities and resources in areas of national and international importance
- Build and maintain state-of-the-art research and teaching facilities
- Attract and support excellent students and postdoctoral fellows

In addition to aligning with Ontario Tech priorities, the Institute also aligns with provincial and federal priorities and action plans on cybersecurity, as outlined in the National Cyber Security Action Plan and the Ontario Cyber Security Framework. It also connects the University to the Ontario information and communications technology sector, which contributes close to $86.6 B in GDP, $193 B in revenue, $11.3 in good exports, $10.6 B in service exports, and employing more than 652 workers in 2018[3]. The Institute will contribute to the ICT sector by creating knowledge, expertise and capacity in the area of cybersecurity through integrating, coordinating and facilitating interdisciplinary research, innovative teaching, and outreach. The Institute will collaborate with partners, and link with accredited programs and schools in the Faculty of Business and Information Technology. Additionally, it will provide an administrative structure for the labs, research and teaching as well as executive education and classes in the Faculty. The Institute aims to be the recognized center of excellence in cyber security, coordinating and leveraging our diverse strengths in Research, Outreach and Experiential Learning.

Research	Training	Outreach
• Supports research threads across all the university, and links to existing centers and institutes inside and outside the university. • Facilitates research into innovative use of technology in teaching • Supports the MSc and PhD research-based program in computer science and related graduate programs of the other faculty members involved in the institute, in	• Supports exchange and partnerships in cyber security related courses • Supports the training for the undergraduate Networking and IT Security (NITS) and the Master of IT Security (MITS) students. • Creates a collaborative over arching training space for future degrees, such as the graduate and undergraduate program in cyber security threat intelligence.	• Focal point for a development plan for 2020 and onward initiatives to help attract innovative donors with sponsorship and naming opportunities • Connections to the community through the creation of an advisory board • Revive the METIS[4] seminar series on cybersecurity topics • Initiate a regional conference

[3]. https://www.ic.gc.ca/eic/site/ict-tic.nsf/eng/h_it07229.html

[4]. The METIS seminar was a first introduced with the inception of the Master of IT Security program and focused on security topics, and was later combined with the general CS graduate seminar

addition to the Master of IT Security program. • Focal point for the application for CFI, NSERC, OCE, SSHRC and other grant applications		

RESOURCES REQUIRED

A. Physical Requirements

Currently, there are a number of research labs in the faculty of Business and Information Technology that can be included under the umbrella of the Institute. These research labs include: The Advanced Networking Technology and Security (ANTS) research lab, the Security, Artificial Intelligence, Networks Lab (SAIN Lab), The Human Machine Lab, the Hackers Research Lab, the Networking Lab, The Finance Lab, the Marketing Lab, the Business Analytics Lab, and the SAP Next-Gen Lab (Labs from other faculties and organizations will be added later). These labs are located in the Software and Informatics Research Centre (SIRC) building, so there are no requirements for renovation or extra hardware. The Institute can definitely benefit from a meeting space, and for that, the Dean of FBIT has agreed to share the current Incubator space in the SIRC building.

B. Staffing Requirements

In addition to a Director for the Institute, who is a full-time faculty member, the Institute will require the help of a full-time Executive Director. This position is very important to coordinate all Institute events and activities, to establish and facilitate connections with industrial partners, to showcase our strength, and to communicate research activities to potential partners and donors. The person in this position will work closely with the Office of External Relations, the Office of Corporate Engagement & Development, as well as the Office of Research Services to build relations and engagements with external partners.

C. Budget and Financial Requirements

The following operational budget proposal is based on a Director for the institute being from extant faculty, with courses covered by LTA, and full-time Executive Director. All incoming money will be raised through grants, service contracts, overhead and fund-raising activities. The budget is aspirational in nature and FBIT will commit to a minimum of the course releases and promotional materials initially. Other items will be subject to fund-raising activities, whereby faculty who benefit from being associated with the Institute will be encouraged to allocate administrative expenses in their grant or research contracts to sustain the Institute over the long term. At this time FBIT and Advancement are actively pursuing funding and naming opportunities for the Institute that could begin as soon as 2020.

Table 1. CSSRS Proposed Budget

Category	Year 1	Year 2	Year 3	Year 4	Year 5
Human Resources					
Director					
Stipend	5,000	5,000	5,000	5,000	5,000
Course Release for (2 courses); to be covered by a sessional instructor	**17,000**	**17,000**	**17,000**	**17,000**	**17,000**
Executive Director (One LTE)§ (including 9% payroll benefits and 3% salary increase every year) (starting salary of $110,000)	59,950	123,497	127,202	131,018	134,948

Administrative Assistant[§] (including 19% payroll benefits and 3% salary increase every year) (starting salary of $45,000)	26,775	55,156	56,811	58,516	60,271
Undergraduate[+] Student(s) (10 hrs a week, with 3% salary increase every year)			13,664	14,074	14,497
Graduate Student(s)[+] (10 hrs a week, with 3% salary increase every year)			19,605	20,194	20,799
Equipment & Supplies					
Laptop (for Exec. Dir.)	4,000				
Colour Printer	500				
Toner, paper, general office supplies	800	800	800	800	800
Promotion (website creation/maintenance; professional printing; business cards)	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**
Seminar Series (travel and accommodation for invited speakers, refreshments,…)		7,500	7,500	7,500	7,500
Travel for Directors (local, national, international conferences)		5,000	6,000	7,000	8,000
Year Total	124,025	223,953	263,582	271,102	278,815
Anticipated Incoming Fund (from overhead, fundraising, joint research grants, service contracts)	125,000	225,000	275,000	300,000	300,000

[§] Please note that the Executive Director and the Administrative Assistant will be hired 6 months from the Institute launching time: the duties of the Executive Director will be carried by the Director during this time, and the duties of the Administrative assistant will be provided by FBIT.

[†] Also note that these graduate and undergraduate students will be hired as part of the Institute, and they will eb in addition to the graduate and undergraduate students hired directly by members of the Institute.

IMPLICATIONS

The Institute for Cybersecurity and Resilient Systems will serve as a central research institute in this field, allowing to pool together and coordinate relevant research activities that are currently scattered around four different faculties, and potentially all faculties at Ontario Tech University. Establishing this Institute will highly increase Ontario Tech University's profile in an area in which the university has established a reputation for excellence and has been highlighted in present (2017-2020) and upcoming (2020-2025) Strategic Research Plan for the university.

The benefits of establishing this Institute includes, but is not limited to: promotion of high-impact interdisciplinary and cross-faculty collaboration in research at the university; enhancing university's profile as a center of excellence in this field; greater support for university researchers, and serving as a magnet for attracting researchers in this field in Canada and abroad. it will also allow the university researchers to pursue larger funding opportunities, to establish formal research networks with other research institutes in Canada and abroad, and to collaborate with agencies such as MITACS, OCE and NSERC in training the next generation of experts in this field.

The Institute will also act as a central point to coordinate and provide highly-needed expertise to governments, businesses, organizations and the public, particularly at the time of emergencies. As an example, during the current COVID-19 pandemic, many organizations and businesses are struggling to move their operations online in a secure and resilient manner, and the Internet backbone itself is being tested under the stress of the sharp spike in online traffic. Issues

of online information privacy, trust and quality have suddenly become an important factor of daily life. The Institute would serve as a consultant to media and government to provide information and expertise about the impact of the pandemic, and to raise awareness about the impact of the pandemic, for instance by conducting and publishing regular assessment of the network resilience and security threats, and to lead research activities with regard to mitigating the negative impacts of the pandemic on people's work and life.

In addition to research activities, it is projected that the Institute will establish a service portfolio to serve the increasing demand from industry. Services such as testing and verification of security products and other service contracts will be high on the list of provided services. Providing the service of testing and verification of security products can be a major source of income to the Institute, in addition to potential opportunity for research engagements and student recruitments.

It is anticipated that members of the Institute will organize a yearly workshop, or symposium on cybersecurity at Ontario Tech University to share some of the research output of the members as well as to raise nationally and internationally the profile of the Institute and the university. The event will also include some industry and training sessions to attract industry and professional personnel to join the event. information about the event, in addition to other research activities and outcomes will be continually published on the Institute’s website.

In addition, it is anticipated that members of the Institute will apply for an NSERC Collaborative Research and Training Experience Program (CREATE) program in the areas related to cybersecurity, information privacy and trust. The collaborative and interdisciplinary approaches to research will increase the chances of receiving the grant. Additionally, some of the donated funds to be received by the Institute will be used to support additional graduate and undergraduate students, and providing these students with additional experiential learning opportunities.

As a research entity within Ontario Tech University, the Institute will follow the same intellectual property and commercialization policy used at the university, which states that the ownership of intellectual property developed using funding from the Institute belongs to the faculty members and students. All businesses that want to partner with the institute will follow the regular process established by the Office of Research Services.

ALIGNMENT WITH MISSION, VISION, VALUES & STRATEGIC PLAN

The Institute for Cyber Security and Resilient Systems aligns with several strategic priority areas of the university, and promotes research on the intersection of technologies, social normal, and businesses that highly impacts the quality of life for human societies, as per University's motto "Tech with a Conscience".

The Institute links to three of Ontario Tech strategic research priorities from the newly released strategic research DRIVING THE FUTURE THROUGH, RESEARCH EXCELLENCE STRATEGIC RESEARCH PLAN, 2020-2025:

1. Data Science, Digital Technologies, and Artificial Intelligence

Majority of the researchers affiliated with the Institute are already integrating various data science approaches, including Artificial Intelligence and Machine Learning techniques to solve big challenges, and this will continue as more and more of these technologies are applied in various

domains. Examples of current projects include applications of big data analytics and machine learning in security, network operations, password management, recommender systems, social media, smart cities and customer data privacy.

2. Autonomous Vehicles and Assisted Mobility

In the past few years, the Automotive Centre of Excellence (ACE) has been attracting various companies interested in security testing and verification of various components of the connected and autonomous vehicles. This shift is expected to continue as more and more computing and communication devices are integrated into vehicles. Various members of the Institute are already working with industry partners on projects related to security and resiliency on future vehicles. Examples of past projects in this area include: privacy implications of connected cars; automotive software security and anomaly detection; context-aware vehicular networks and smart road-sensing technologies.

3. Social Innovation, Disruptive Technologies, and the New Economy

As new technologies continue to change businesses and social norms, an inter-disciplinary evaluation of how these norms can be disrupted by security attacks and how developed solutions can be introduced and adopted. The inter-disciplinary background of the researchers in the institute will allow for innovative design and evaluation of how new technologies can be designed to improve security and increase resiliency. Examples of the projects by the institute's researchers include the widely-reported companion robots which was featured in major media stories; the AI-with-empathy project; Legal and social research on digital piracy and cyber-bullying; Children's privacy protection for smart toys; behavioural information security; fraud prevention; device comfort, and Human-AI trust relationships.

The institute will also promote and contribute to the university's mission in regard to the training of students and HQPs. All faculty members associated with the Institute have a strong track record of supervising graduate and undergraduate students, as well as post-doctoral fellows. It is expected that the institute will facilitate co-supervision from multiple faculties. This will provide faculty members from faculties that do not have graduate students to access and supervise graduate students from other faculties in the target areas.

The institute will leverage the high number of current applications to the Master of IT Security (MITS) program in FBIT, in addition to the undergraduate program in Networking and IT Security, to start other specializations in addition to the existing specialization in Artificial intelligence. Some of these specializations will include Information Technology Audit and Compliance, Risk Management and Business Continuity, Cyber Crime and Fraud Investigation, Industrial Control Systems Security, Incident Response, and Forensic Analysis. Some of the developed courses for these specializations can also be used to create a wide range of Graduate Certificates.

ALTERNATIVES CONSIDERED:

N/A

CONSULTATION:

Lots of consultation went into the development of the proposal for the Institute for Cyber Security and Resilient Systems (ICSRS), including:

- *Office of Research Services*: May 2019 – present
- *Internal researchers*: Discussions have been taking place between all researchers in the proposals.

- *External potential partners*: Discussions already going on with CIBC and Check point to support the Institute. Other discussions are planned with IBM in the near future.
- Discussions with members of the Networking and IT Security Advisory Board.
- *FBIT Faculty council*: Motion passed April 14, 2020
- *Research Board*: Motion passed April 24, 2020

COMPLIANCE WITH POLICY/LEGISLATION:
The Institute for Cyber Security and Resilient Systems (ICSRS) proposal was developed in conjunction with the Office of Research Services to align with the University's Procedure for the Creation of Research Units, Centres and Institutes (see Appendix 1).

NEXT STEPS:
Send the proposal to the Board of Governors for approval.

MOTION FOR CONSIDERATION:

That pursuant to the recommendation of the Research Board, Academic Council hereby recommends the establishment of the Institute for Cyber Security and Resilient Systems (ICSRS) for approval by the Board of Governors, as presented.

SUPPORTING REFERENCE MATERIALS:

1. Full proposal for the creation of the Institute for Cyber Security and Resilient Systems (ICSRS) at Ontario Tech University

Institute for Cyber Security and Resilient Systems (ICSRS)

I. Name of the Entity

Institute for Cyber Security and Resilient Systems (ICSRS)

II. Proposers:

A. Director

Khalil El-Khatib, PhD
Professor, Faculty of Business and Information Technology
Khalil.el-khatib@ontariotechu.ca

B. Co-Proposers (In Alphabetical Order)

- Amirali Abari, Faculty of Business and Information Technology
- Rajen Akalu, Faculty of Business and Information Technology
- Shahram S. Heydari, Faculty of Business and Information Technology
- Patrick Hung, Faculty of Business and Information Technology
- Stephen Jackson, Faculty of Business and Information Technology
- Fletcher Lu, Faculty of Business and Information Technology
- Stephen Marsh, Faculty of Business and Information Technology
- Miguel Vargas Martin, Faculty of Business and Information Technology
- Julie Thorpe, Faculty of Business and Information Technology

C. Affiliated Faculty Members (In Alphabetical Order)

- Akramul Azim, Faculty of Engineering and Applied Science
- Steven Downing, Faculty of Social Science and Humanities
- Les Jacob, Vice-President, Research and Innovation
- Qusay Mahmoud, Faculty of Engineering and Applied Science
- Christopher O'Connor, Faculty of Social Science and Humanities
- Richard Pazzi, Faculty of Business and Information Technology
- Andrea Slane, Faculty of Social Science and Humanities
- Ed Waller, Faculty of Energy Systems and Nuclear Science

III. Background Description and Justification

There has been a sharp increase in the number of cyberattacks over the last few years, costing businesses trillions of dollars, in addition to the loss of billions of personal and financial records (and possible meddling with elections) [1]. Recent advancement in computation and communication, coupled with the proliferation of the Internet and the rush to replace physical systems with more digitally enabled systems have made cybersecurity an international challenge. What is even more important is that the threat landscape has changed over the last few years; the increase in state-sponsored attacks shows that governments around the world have been investing in cybersecurity capabilities.

While the majority of public and private organizations use various solutions to protect themselves from potential cyberattacks, there is rarely a day that we do not hear news about cyber security incidents. Whether it is ransomware, distributed denial of service (DDOS), phishing or spear phishing, drive-by, password SQL injection, eavesdropping, social engineering or any other form of attack, these attacks are inflecting havoc on various sectors of the Canadian economy (more than $3 billion in economic losses each year [2]). Some of these attacks also inflicted damages on the lives of millions of Canadians. In November 2019, threat actors managed to infect all Nunavut government electronic services with a ransomware that paralyzed all operations. A number of Ontario municipalities (Stratford, Woodstock and The Nation) were also hit with ransomware attacks. Ransomware hit three Ontario hospitals crippling their computer system and locking access to patients' medical data. In August 2019, the Five Eyes alliance that includes Canada, the United States, New Zealand, Australia, and the UK, accused China of running a 12-year campaign of cyber espionage to steal trade secrets and intellectual properties from companies in 12 countries around the world. In December, security researchers from Palo Alto Networks attributed a campaign to infect various government agencies in four continents with malware to the Russian cyber-espionage group Sofacy.

Cyberspace is a unique environment where IT, business and people intertwined together, making it a challenge to systematically enforce procedures and maintain security. It is common knowledge in cybersecurity that the single weakest link in the information security chain is always the human being, and that most of the cybersecurity incidents are the results of human actions (or inactions). Therefore, in order to improve security in cyberspace, it is important to factor the human aspect of any security solution. Ensuring a secure and robust cyberspace requires a solid understanding of human nature and its role in the whole cyberspace ecosystem; factors such as the acceptability of cyber policies and controls, understanding the motivations behind cyberattacks, the background of cyber victims and criminals, and identifying and eliminating insider threats are all challenges rooted in social and behavioral science.

The traditional view of cybersecurity in a binary form (secure vs. insecure, verified vs. unverified etc.) is also changing rapidly. An emerging paradigm focuses on the concept of *trust* as the basic description of an entity's reliability, performance and security. A trust-based cyberspace

---

1. TrendMicro - Unseen Threats, Imminent Losses - 2018 Midyear Security Roundup. Available at https://documents.trendmicro.com/assets/rpt/rpt-2018-Midyear-Security-Roundup-unseen-threats-imminent-losses.pdf. Accessed on Oct 17, 2018.
2. National Cyber Security Action Plan (2019-2024) Available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx

can be described as an infrastructure for information exchange in which the accuracy, integrity and confidentiality of information are not deterministic and binary, but instead are based on a dynamic trust score. Such trust scores can be assigned to multiple different network entities, which can be are based on multitude of factors based on reputation, reliability, performance and past history. Such trust scores are both subjective and dynamic: an action, lack of action or state change could alter, and even potentially rescind the trustworthiness of an entity inside or outside the cyberspace. This new paradigm will form the basis for a *resilient* cyberspace, in which every entity (physical, logical, or information) is evaluated dynamically and constantly based on the events in the cyberspace, and actions/decisions are taken to maintain or improve the cyber resilience in face of those events.

Along with resilience, the issue of privacy has also become one of the most important topics of discussion today. For a majority of consumers, getting better services in a digital economy may be worth sacrificing the confidentiality of some private data by making it available to service providers or to the public, as long as they can trust the ability of the service provider to keep it safe. However, there are few alternatives for those who may prefer to have a choice in this matter and control what information they provide to the companies. The current deployment of technology does not provide many choices to such customers. Whether people want or not, their utility usage, internet access, cell phone location and vehicle information is collected and maintained individually by service providers, making an anonymous life impossible. As more advanced technologies for smart cities are developed, maintaining such anonymity becomes harder.

The concept of anonymization or de-identification on the Internet has long been studied, and solutions such as web anonymizers have been around for many years. Such services often work based on aggregation and randomization in which user data from many sources are combined to de-identify individual sources, providing a degree of collective anonymity. In the area of smart city utilities, the concept of "Privacy-by-Design" has been introduced as a potential solution to maintain privacy of consumer data. In this model, the manufacturers of utility devices and service providers must work together to design their systems to operate with no or minimal reliance on individual consumer data. The use of aggregated smart meter readings and data de-identification tools is encouraged in system design.

Addressing all these important questions will provide challenges for researchers in the field of information security for years to come. Many researchers at Ontario Tech university are currently studying various aspects of cybersecurity, trustable networks and information privacy. The objective of this proposal is to provide a focal point for coordinating research work in this interdisciplinary area, to pool resources together, and to attract external funding for this area of research.

IV. The need for an interdisciplinary approach to address the challenges to cybersecurity and resiliency

Cybersecurity is a multifaceted challenge that combines technologies, people and social normal, and spans multiple sectors. And while cybersecurity is considered a subfield of information technology, it has strong relations to other disciplines, especially the fields of business and social science, which indicates that impactful cybersecurity solutions necessitate collaborative approaches across multiple disciplines and practices.

For instance, the term "cyberaggression" defined by Harknett *et. al.*, is used "to capture the range of activities associated with disruptive computer hacking, cybercrime, cyberespionage, cyberconflict, and cyberwar recognizing that each of those terms provides greater precision to specific realms of aggression." [3] it is not hard to see that most of these forms of aggressions are close imitations of the same aggressions that happen in the real world, except that they use the information technology platform. These forms of aggressions are well researched in the fields of criminal justice and political science, with well established detection and response techniques that can be adopted and modified in the cyber world. [4] These related fields go even deeper than the typical approaches taken in cybersecurity, to even study the root causes of these aggressions.

Understanding researches and theories in behavior science can also help improve cyber security and reduce risks. Sasse and Flechais pointed out that in order to "prevent users from being the 'weakest link,'" one must have a good understanding of behavioral science. [5] Both Predd *et al.* [6], 2008; Pfleeger *et al*. [7] emphasised the importance of understanding human behaviors as well when designing, developing, deploying and using cyber security. The linkage between behavioral science and security is clear when it comes to how people trust to mitigate risk when they are online, and even when building automated multi-agent systems. Additionally, there is a large body of knowledge in behavior science that relate decision making, employee compliance and deviance to the risk level of an organization [8].

Cybersecurity is intertwined with the way business and government operate, and it is hard to separate the cause and effect of the two areas. And while the impact of cybersecurity on business is well researched, various business fields can also be leveraged to address security challenges. For instance, research findings in the field of economics can be used to find a balanced resource allocation point between a viable business and secure organization. Research methods from the field of human resources and organizational behavior can help hire and retain loyal people, and minimise the risks of insiders' threat. Marketing field can help introduce security solutions into organizations and persuade them to see these new technologies as enablers, and not inhibitors.

Today, a large, yet fragmented, number of research activities related to cyber security is done by a number of researchers and in different research labs, with a large concentration of security, privacy and trust happening within the Faculty of Business and Information Technology, with a fairly large number of social science research happening with the Faculty of Social Science and Humanities (FSSH), in addition to some research on software security happening within the Faculty of Engineering and Applied Science (FEAS), and nuclear physical security happening in the Faculty of Energy and Nuclear Science (FENS).

Though Ontario Tech University is a small university, most of the research still happens in silos. The main objective of the proposed institute is to create a fertile ground for potential collaboration between researchers from different disciplines. More specifically, the Institute will allow researchers to:

- Create opportunities for researchers to network and share ideas.
- Address bigger challenges in cybersecurity and make larger and impactful solutions to society.
- Allow faculty members from faculties that do not have graduate programs to participate in student supervision.
- Leverage the power of an institute when applying for individual or large grants (Canada Foundation for Innovation, NSERC Collaborative Research and Training Experience Program (CREATE), NSERC Networks of Centres of Excellence (NCE), New Frontiers in Research Fund, SSHRC Partnership grants.

V. Research Mandate

One of the institutional priorities for Ontario Tech is "Tech with a conscience" which is defined as the responsible and ethical use and development of technologies that can help with the progress and prosperity of humanity. As today's technology is intertwined with the daily artifacts and applications spanning multiple domains, it is imperative to tackle the human-business-technology challenge from an interdisciplinary perspective. Being at the front of research and use of technology, and with a large concentration of faculty members carrying leading-edge research in Information Technology (Security, Privacy, Trust) and Social Science (business, law and ethics), Ontario Tech is strategically situated for developing and evaluating the impact of new technologies on our society. Being a small and innovative university, and with many cross-appointments and collaborations between many faculty members, establishing a research institute will provide the rich environment to cultivate and promote research on the influence of new security, privacy and trust technologies on human and society, as well as guiding the design and development of future technologies.

The Faculty of Business and Information Technology has taken a major initiative to develop a cybersecurity research institute, called the Institute for Cyber Security and Resilient Systems (ICSRS), with a mandate to research the intersection of technical, legal, social, economic and ethical implications of privacy, security and trust technologies. The institute will create a focal point within Ontario Tech University, for research, teaching, and outreach in the field of cyber security protection (e.g. critical infrastructure protection, identity management, protection from

---

3. Harknett, R. J., Callaghan, J. P., & Kauffman, R., Leaving Deterrence Behind: War-Fighting and National Cybersecurity. Journal of Homeland Security and Emergency Management, 7(1), 22 (2010), 1-24.
4. Stockman, Mark. "Infusing social science into cybersecurity education." Proceedings of the 14th annual ACM SIGITE conference on Information technology education. 2013.
5. Sasse, M. Angela and Ivan Flechais, "Usable Security: Why Do We Need It? How Do We Get It?," in Lorrie Faith Cranor and Simson Garfinkel, eds., Security and Usability, O'Reilly Publishing, Sebastopol, CA, 2005, pp. 13-30.
6. Predd, Joel, Shari Lawrence Pfleeger, Jeffrey Hunker and Carla Bulford, "Insiders Behaving Badly," IEEE Security and Privacy 6(4), July/August 2008, pp. 66-70.
7. Pfleeger, Shari Lawrence, Joel Predd, Jeffrey Hunker and Carla Bulford, "Insiders Behaving Badly: Addressing Bad Actors and Their Actions," IEEE Transactions on Information Forensics and Security, 5(2), March 2010.
8. Klein, Gary A. and Eduardo Salas, eds., Linking Expertise and Naturalistic Decision Making, Erlbaum, 2001.

social engineering, secure software system, password protection, …) to enhance online and offline cyber protection and innovation. The focus of the Institute will be broadly to examine issues surrounding the use and protection of emerging technologies in both public and private sectors. The Institute links to three of Ontario Tech strategic research priorities from the newly released strategic research DRIVING THE FUTURE THROUGH, RESEARCH EXCELLENCE STRATEGIC RESEARCH PLAN, 2020-2025. The Institute would address the following Ontario Tech priorities:

- Attract and retain outstanding national and international academics
- Place priorities and resources in areas of national and international importance
- Build and maintain state-of-the-art research and teaching facilities
- Attract and support excellent students and postdoctoral fellows

In addition to aligning with Ontario Tech priorities, the Institute also aligns with provincial and federal priorities and action plans on cybersecurity, as outlined in the National Cyber Security Action Plan and the Ontario Cyber Security Framework. It also connects the University to the Ontario information and communications technology sector, which contributes close to $86.6 B in GDP, $193 B in revenue, $11.3 in good exports, $10.6 B in service exports, and employing more than 652 workers in 2018[9]. The Institute will contribute to the ICT sector by creating knowledge, expertise and capacity in the area of cybersecurity through integrating, coordinating and facilitating interdisciplinary research, innovative teaching, and outreach. The Institute will collaborate with partners, and link with accredited programs and schools in the Faculty of Business and Information Technology. Additionally, it will provide an administrative structure for the labs, research and teaching as well as executive education and classes in the Faculty. The Institute aims to be the recognized centre of excellence in cyber security, coordinating and leveraging our diverse strengths in Research, Outreach and Experiential Learning.

Research	Training	Outreach
• Supports research threads across all the university, and links to existing Centres inside and outside the university. • Facilitates research into innovative use of technology in teaching • Supports the MSc and PhD research-based program in computer science and related graduate programs of the other faculty	• Supports exchange and partnerships in cyber security related courses • Supports the training for the undergraduate Networking and IT Security (NITS) and the Master of IT Security (MITS) students. • Creates a collaborative over arching training space for future degrees, such as the graduate and undergraduate	• Focal point for a development plan for 2020 and onward initiatives to help attract innovative donors with sponsorship and naming opportunities • Connections to the community through the creation of an advisory board • Revive the METIS[10] seminar series on cybersecurity topics

9. https://www.ic.gc.ca/eic/site/ict-tic.nsf/eng/h_it07229.html

10. The METIS seminar was a first introduced with the inception of the Master of IT Security program and focused on security topics, and was later combined with the general CS graduate seminar

members involved in the institute, in addition to Master of IT Security program. • Focal point for the application for CFI, NSERC, OCE, SSHRC and other grant applications	program in cyber security threat intelligence.	• Initiate a regional conference

VI. ICSRS Programs and Activities

Within the first two years, the objective of the institute will focus on a rapid start of activities that focus on creating an infrastructure and relationships within and outside the institute. With the help of various parties at the university, members of the institute will also be involved in a fundraising program to raise money to support the institute activities. The details of these programs and activities are included below.

A. Build Institute Governance Body, Infrastructure and Relationships

- Create an ICSRS Advisory Board (around 10 members) consisting of thought leaders in digital innovation with strong connections or senior level positions in the industry.
- Create a steering committee (6-7 members) from faculty members within the institute representing the various area of interest.
- With the help of the Office of Research Services, the steering committee will develop an internal governance body, responsibilities, procedures and processes for overseeing the institute activities, including the process of allocating money raised through funding activities, reporting structure, scheduling regular meetings, to mention a few.
- If needed, refine the preliminary structure of the governance body of the institute, as shown in Figure 1.
- Create material about research expertise and capabilities.
- Revive the FBIT Metis Seminar Series on Cybersecurity.
- Pursue research funding in partnership with private and public sector partners.
- Organise inter-disciplinary funding development workshops.
- Foster and develop inter-university relationships and funding proposals potential venue for funding proposal includes: NSERC, SSHRC, CFI, MITACS, and OCE.

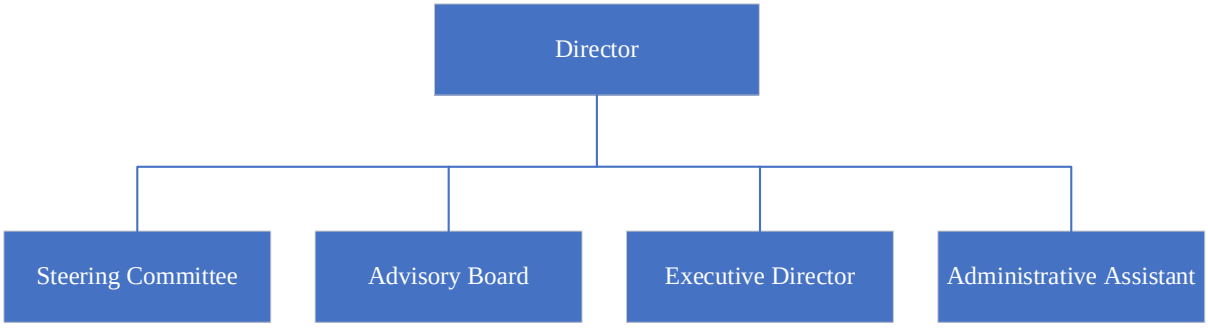

Figure 1. Preliminary structure for governance body

B. Fundraising

The institute director will work with the Advancement Office at Ontario Tech to develop a plan for initiatives to help attract donors and sponsors. Potential fundraising campaigns will target:

- IBM
- McAfee
- Trend Micro
- The Herjavec Group
- TD
- Accenture
- CIBC
- KPMG
- RBC
- Pricewaterhous eCoopers
- Meridian
- Deloitte Canada
- Bell
- SunLife
- Telus
- NortonLifeLock Inc. (Symantec)
- Rogers
- Checkpoint
- Spirent
- Security Compass
- Splunk

Many faculty members have existing relationships with some of these organizations. Additionally, a lot of these organizations already employ some of the faculty alumni, which would help make the case for asking for donations.

The money raised from the fundraising activities will be used to:

- Support interdisciplinary research and innovation in cybersecurity
- Support graduate research assistantship for graduate students
- Create a number of scholarships for graduate and undergraduate students
- Provide support for cybersecurity-focused start-up companies, in conjunction with the brilliant catalyst and the spark center
- Purchase new equipment for the research labs
- Work with university regional partners such as Oshawa Chamber of Commerce and Whitby Chamber of Commerce to support small and start-up businesses with cybersecurity challenges
- Initiate a new major/concentration/specialization in our undergraduate programs (DecSecOps, Security for Industrial Control System)
- Create new professional training and certification programs, in addition to the existing MITS program (examples include Graduate Certificate in Information Technology Audit and Compliance, Risk Management and Business Continuity, Cyber Crime and

Fraud Investigation, Industrial Control Systems Security, Incident Response, and Forensic Analysis.

- Sponsor seminar series on campus and on premise
- Support the on-going cybergirls events, and expand it to high school students
- Sponsor students' clubs and activities
- Cover for the salary of the Executive Director of the Institute
- Cover for the expenses (stipend and course release) for the Director of the Institute

VII. Resource Requirements

A. Physical Requirements

Currently, there are a number of research labs in the faculty of Business and Information Technology that can be included under the umbrella of the Institute. These research labs include: The Advanced Networking Technology and Security (ANTS) research lab, the Security, Artificial Intelligence, Networks Lab (SAIN Lab), The Human Machine Lab, the Hackers Research Lab, the Networking Lab, The Finance Lab, the Marketing Lab, the Business Analytics Lab, and the SAP Next-Gen Lab (Labs from other faculties and organizations will be added later). These labs are located in the Software and Informatics Research Centre (SIRC) building, so there are no requirements for renovation or extra hardware. The institute can definitely benefit from a meeting space, and for that, the Dean of FBIT has agreed to share the current Incubator space in the SIRC building.

B. Staffing Requirements

The institute will require the help of a full-time Executive Director. This position is very important to coordinate all Institute events and activities, to establish and facilitate connections with industrial partners, to showcase our strength, and to communicate research activities to potential partners and donors. The person in this position will work closely with the Office of External Relations, the Office of Corporate Engagement & Development, as well as the Office of Research Services to build relations and engagements with external partners.

C. Budget and Financial Requirements

The following operational budget proposal is based on a Director for the institute being from extant faculty, with courses covered by LTA, and full-time Executive Director. All incoming money will be raised through grants, service contracts, overhead and fund-raising activities. The budget is aspirational in nature and FBIT will commit to a minimum of the course releases and promotional materials initially. Other items will be subject to fund-raising activities, whereby faculty who benefit from being associated with the Institute will be encouraged to allocate administrative expenses in their grant or research contracts to sustain the Institute over the long term. At this time FBIT and Advancement are actively pursuing funding and naming opportunities for the Institute that could begin as soon as 2020.

Table 1. CSSRS Proposed Budget

Category	Year 1	Year 2	Year 3	Year 4	Year 5
Human Resources					
Director					
Stipend	5,000	5,000	5,000	5,000	5,000
Course Release for (2 courses); to be covered by a sessional instructor	**17,000**	**17,000**	**17,000**	**17,000**	**17,000**
Executive Director (One LTE)§ (including 9% payroll benefits and 3% salary increase every year) (starting salary of $110,000)	59,950	123,497	127,202	131,018	134,948
Administrative Assistant§ (including 19% payroll benefits and 3% salary increase every year) (starting salary of $45,000)	26,775	55,156	56,811	58,516	60,271
Undergraduate† Student(s) (10 hrs a week, with 3% salary increase every year)			13,664	14,074	14,497
Graduate Student(s)† (10 hrs a week, with 3% salary increase every year)			19,605	20,194	20,799
Equipment & Supplies					
Laptop (for Exec. Dir.)	4,000				
Colour Printer	500				
Toner, paper, general office supplies	800	800	800	800	800
Promotion (website creation/maintenance; professional printing; business cards)	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**
Seminar Series (travel and accommodation for invited speakers, refreshments,…)		7,500	7,500	7,500	7,500
Travel for Directors (local, national, international conferences)		5,000	6,000	7,000	8,000
Year Total	124,025	223,953	263,582	271,102	278,815
Anticipated Incoming Fund (from overhead, fundraising, joint research grants, service contracts)	125,000	225,000	275,000	300,000	300,000

§ Please note that the Executive Director and the Administrative Assistant will be hired 6 months from the Institute launching time: the duties of the Executive Director will be carried by the Director during this time, and the duties of the Administrative assistant will be provided by FBIT.

† Also note that these graduate and undergraduate students will be hired as part of the Institute, and they will eb in addition to the graduate and undergraduate students hired directly by members of the Institute.

VIII. Proposed Staffing Model for ICSRS

The initial staffing model of ICSRS would consist of a **Director** and a newly appointed full-time **Executive Director**. Initial admin support (for the first 6 months) will be provided by existing faculty staff, with a full-time person hired in the position afterward when funding is released.

The **Director** will:

- Report to the Dean of the Faculty of Business and Information Technology
- Lead fundraising initiatives
- Champion ICSRS internally and externally, and encourage and enhance pursuit of interdisciplinary research grant applications related to the objectives of ICSRS
- Lead the development and operation of ICSRS as an excellent applied research and outreach organization
- Provide leadership and support to the staff and faculty affiliates of the Institute
- Coordinate ICSRS's outreach activities and interact with external bodies (funding agencies, media, other research organizations, and the public)
- With the help of FBIT PBO, administer funding and in-kind contributions provided in accordance with budgets approved by Ontario Tech University's financial accountability policies
- Oversee conferences as per the funding plan
- Promote ICSRS and the work of its affiliate researchers at local, national, and international conferences, and to the media

Reporting to the **Director,** the **Executive Director** will:

- Initiate and maintain relationships with potential partners in the private and public sector in conjunction with the Director
- Create and manage ICSRS's marketing and communication strategy
- Operate the day-today operations of the Institute
- Research alumni for targeted marketing and help source funding and manage finances
- Assist with writing funding proposals
- Liaise with other internal and external research centres (e.g., OTU Concordia, Carleton, UNB)
- Help the Director preparing the budget for the Institute and maintain financial records in accordance with Ontario Tech policy
- Coordinate ICSRS conferences, meetings and events
- Create and maintain ICSRS website and social media presence

It is important that the Executive Director holds a graduate degree in a field related to cybersecurity, and with some experience in industry liaison.

IX. Student Involvement and Training

All faculty members associated with the Institute have a strong track record of supervising graduate and undergraduate students, in additional to post doc fellows. It is anticipated that these faculty members will continue do that, but it is expected that the institute will enable co-supervision from multiple faculties. This will provide faculty members from faculties that do not have graduate students to access and supervise graduate students that are available in other faculties. In addition, it is anticipated that members of the Institute will apply for an NSERC Collaborative Research and Training Experience Program (CREATE) program in cybersecurity. The collaborative and interdisciplinary approaches to research will increase the chances of

receiving the grant. Additionally, some of the donated funds to be received by the institute will be used to support additional graduate and undergraduate students, and providing these students with additional experiential learning opportunities.

The institute will leverage the high number of current applications to the Master of IT Security (MITS) program in FBIT, in addition to the undergraduate program in Networking and IT Security, to start other specializations in addition to the existing specialization in Artificial intelligence. Some of these specializations will include Information Technology Audit and Compliance, Risk Management and Business Continuity, Cyber Crime and Fraud Investigation, Industrial Control Systems Security, Incident Response, and Forensic Analysis. Some of the developed courses for these specializations can also be used to create a wide range of Graduate Certificates.

X. Research Dissemination and Service Plan

It is anticipated that members of the institute will organize a yearly workshop, or symposium on cybersecurity at Ontario Tech University to share some of the research output of the members as well as to raise nationally and internationally the profile of the institute and the university. The event will also include some industry and training sessions to attract industry and professional personnel to join the event. information about the event, in addition to other research activities and outcomes will be continually published on the institute's website.

In additional to research activities, it is projected that the institute will establish a service portfolio to serve the increase demand from industry. Services such as testing and verification of security product and other service contracts will be high on the list of provided services. Providing the service of testing and verification of security product can be a major source of income to the institute, in addition to potential opportunity for research engagements and student recruitments.

XI. Intellectual Property and Commercialization

As a research entity within Ontario Tech University, the institute will follow the same intellectual property and commercialization policy used at the university, which states that the ownership of intellectual property developed using funding from the institute belongs to the faculty members and students. All business that want to partner with the institute will follow the regular process establish by the Office of Research Services.

Appendix A. Researchers and Research Facilities

The Institute for Cyber Security and Resilient Systems includes researchers and research facilities from different faculties. Below is the list of these faculty members, some of their cybersecurity related research projects and research facilities.

A. Bios for All Researchers Included in the Institute (In Alphabetical Order)

Each of the following faculty members has been involved in cyber security related research activities. While the list might not be complete, it can potentially grow as more faculty members learn about the institute and get involved with it. The faculty members are listed in alphabetical order:

1) Amirali Abari, FBIT

Amirali Abari is an Assistant Professor in the Faculty of Business and Information Technology at Ontario Tech University. Prior to that, he was an NSERC Postdoctoral Fellow, with a joint appointment at the University of Toronto and University of Waterloo. He received his Ph.D. in Computer Science from the University of Toronto in 2016. His research interests have spanned a wide range of topics including machine learning, multi-agent systems, computer security, and privacy. His current research focus lies in designing, exploring, and extending the capabilities of *user-centered intelligent systems* for improving our well-being and protecting our security and privacy. His research has appeared in top-tier CS venues, received a student best paper award (IEEE PST 2010), been granted a US patent, and been generously funded by NSERC, SSHRC, and many others in combination of research grants and fellowships. He has served on the conference program committees of leading international conferences in Artificial Intelligence such as AAAI, IJCAI, AAMAS. He also frequently reviews for top journals in Artificial Intelligence, Algorithms, and Computer Security including IEEE Transactions on Knowledge and Data Engineering, Journal of Artificial Intelligence Research, ACM Transactions on Spatial Algorithms and Systems, Algorithmica, and IEEE Transactions on Information Forensics & Security.

Some of Dr. Amirali's current project include:

- AI-Empowered Password Guessing and Meters (current). The objective of this project is to evaluate the effectiveness of password guessing tools for a realistic assessment of the security of passwords. The project includes a large-scale study of six well-known password guessers/cracking methods with six leaked password datasets.
- Unlocking Recommender Systems for Privacy and Security Domains (current). The objective is to design and develop artificial intelligence (AI) algorithms, technologies, and systems that pave the way for the development of recommendation systems for high-impact privacy and security decisions.
- AI-Assisted Attacks on Graphical Passwords (Past). This project studied users' graphical password decision processes by visual attention models for capturing how humans cognitively process images. The project developed as well artificial intelligence techniques for security assessment of a particular type of graphical passwords, called Passpoints.
- Geographical Authentication (Past). The project proposed, designed, implemented, and evaluated a novel idea for user authentication that we call location-passwords a digital-map based form of user authentication where a user chooses a place as their password.

- Video-Passwords: Authentication while Advertising (Past). The project introduced video-passwords, a novel class of user authentication schemes that involves the user watching and remembering parts of a given video as their password.
- Measuring and Quantifying Known Adversaries (Past). This project developed three models, inspired by Social Psychology literature, to quantify the known adversary in paired user studies, and test them using a case study.

2) Rajen Akalu, FBIT

Rajen Akalu is an assistant professor in the Faculty of Business and Information Technology at Ontario Tech University in Oshawa. His research interests as well as law firm practice areas relate to information privacy law and new technologies. In 2014 he completed his Ph.D. at Delft Technical University (TU Delft), The Netherlands on the regulation of wireless technology. Rajen holds a Master of Laws degree from the London School of Economics and a Bachelor of Laws degree from the University of East London. Rajen is called to the Bar in Ontario. He is an executive member of the Privacy and Access section of the Ontario Bar Association and a member of the International Association of Privacy Professionals (IAPP). Rajen previously worked at the Center for Information Communication Technologies, Denmark Technical University and the Centre for Innovation Law and Policy, University of Toronto Faculty of Law. He has also worked in law firms in New York and Toronto as well as the Information Privacy Commissioner (Ontario) and the Commission for Communications Regulation (ComReg), Ireland. His current research on the privacy implications of connected and automated vehicles was funded by the Office of the Privacy Commissioner of Canada.

Some of Dr. Rajen's current project include

- "Paving the way for Intelligent Transport Systems (ITS): The Privacy Implications of Vehicular Infotainment Platforms." This project focuses on information privacy specifically related to infotainment platform in connected vehicles
- "Developing a Privacy Code of Practice for the Connected Car" This project develop a code a practice based on the CSA model code found in the PIPEDA.

3) Akramul Azim, FEAS

Dr. Akramul Azim is currently an Assistant Professor in software engineering at Ontario Tech University. He completed his PhD from University of Waterloo and he has professional experience working with Ericsson Canada, BlackBerry QNX, Quanser, and Huawei. He is also a professional engineer of Ontario and senior member of IEEE. He is currently leading the Real-Time EMbedded SOFTware (RTEMSOFT) research lab at Ontario Tech University. Dr. Azim's areas of research include verification and validation of software systems, software testing, security and safety of systems software, embedded software and internet of things. In these areas, Dr. Azim has many research publications in top conferences and journals including two patents.

Some of Dr. Azim's past and current project include:

- Jammed area mapping of wireless sensor networks
- Automotive software security
- Anomaly detection
- Container security
- Security by design for embedded systems

4) Khalil El-Khatib, FBIT

Dr. El-Khatib was an assistant professor at the University of Western Ontario prior to joining Ontario Tech University in July 2006. Between 1992 and 1994, he worked as a research assistant in the Computer Science department at American University of Beirut. In 1996, he joined the High Capacity Division at Nortel Networks as a software designer. From February 2002, he was a research officer in the Network Computing Group (lately renamed the Information Security Group) at the National Research Council of Canada (NRC) for two years, and continued to be affiliated with the group for another two years. Today, Dr. El-Khatib is a full professor and the co-director or the Advanced Networking Technologies and Security (ANTS) at Ontario Tech. His research interests include:

Some of Dr. El-Khatib current project include:

- Threat Analysis of a Long Range Autonomous Unmanned Aerial System: The objective of this work is to provide an overview of autonomous UAS architecture and analyzes security threats to the system. The goal of this paper is to support UAV manufacturers and developers to understand the components required in an autonomous UAS and allow them to identify, prevent and address security concerns within their systems.
- A Framework for Assessing the Robustness of Natural Language Processing Classifiers: The objective of this work is to introduce a framework to increase the robustness of NLP classifiers. The framework uses genetic algorithms to attack classifiers with adversarial texts with the purpose of identifying robustness issues in the classifiers.
- Malware detection and threat hunting methods based on environmental data: This work is an attempt to investigate another malware research method that could be useful in large enterprises where majority of the IT tasks are automated and performed by authorized systems and systems designed to be as homogeneous as possible
- Insider Threat Prevention Using Big Data Analytics: In this research work, we studied and were the first to establish the possibility of using the user's intention as an access control measure by studying the involuntary electroencephalogram reactions toward visual stimuli. We also proposed intent-based access control (IBAC) that detects the intentions of access based on the existence of knowledge about an intention.
- Measuring Privacy: The work proposed an original model of the states of privacy based on the identifiability of an individual. Representation is a finite state machine, while the same list of factors can be used to calculate transitions in the machine.
- Privacy Enhancing Technologies for Smart Cities: This work provided a critic review of the state of Smart Cities around the world, some examples of implemented solutions, and then further explores how the privacy of individuals could be exposed and how this exposure could be mitigated using multiple privacy enhancing technologies.
- Big Data Analytics Architecture for Security Intelligence: Using big data analysis algorithm for social media data, the work presented the design and implementation of an architecture to determine phishing susceptibility of a user through their social media accounts, and methods to reduce the threat. Building on our initial work, we explored some of the existing architectures for big data intelligence analytics, and proposed an architecture that promises to provide greater security for data intensive environments.

5) Steven Downing, FSSH

Dr. Steven Downing received his PhD in Criminology from The University of Texas at Dallas, where he also received a Master of Arts in Sociology. He has applied theories of crime to online settings, where he qualitatively examines subcultural and social control constructs surrounding deviant and criminal behaviour such as digital piracy and cyber-bullying. He also explores methodological issues surrounding online ethnography, interviewing and other qualitative approaches.

Some of Dr. Steven work include:

- Technology & Crime Prevention
- "Selfie": Cyber-bullying Theory and the Structure of Late Modernity.
- Nonconsensual Intimate Image Sharing: A Perception Analysis
- Bullying Enters The 21st Century? Turning a Critical Eye to Cyberbullying Research.
- Retro Gaming Subculture and the Social Construction of a Piracy Ethic.
- Social Control in a Subculture of Piracy.
- Attitudinal and Behavioral Pathways of Deviance in Online Gaming

6) Shahram Heydari, FBIT

Shahram Shah Heydari is an Associate Professor in the Faculty of Business and Information Technology, University of Ontario Institute of Technology (Ontario Tech), Canada. Prior to joining Ontario Tech in 2007, he was a System Engineer and Member of Scientific Staff at Nortel Networks where he worked on element management in ultra high-speed IP/MPLS routers, performance modeling of automatically switched optical networks (ASON), and proprietary voice-over-IP transport control protocols. His main research interests include network design and planning, software-defined networking, applications of Artificial Intelligence (AI) in network management, and network Quality of Experience (QoE). He received his B.Sc. and M.Sc. degrees in Electronic Engineering from Sharif University of Technology (Iran), M.A.Sc. degree from Concordia University, Montreal, and Ph.D. degree from University of Ottawa, Canada.

Some of Dr. Heydari current project include:

- Predictive Cybersecurity Architecture: The key objective of this project is to develop an AI-based predictive model of security attacks for telecommunication networks.
- Protecting Critical Infrastructure against Large-Scale Failures and attacks: The main objectives of this research were to analyze the impact of large-scale failure scenarios arising from security attacks or natural disasters on the telecommunication infrastructure, and to design multi-layer restoration schemes, methods and algorithms for integrated protection and traffic restoration of access, metropolitan and backbone layers of the network.
- Middleware For Smart Critical Infrastructure Networks Intercommunication: The objective of this research was to develop a uniform framework for information exchange between heterogenous critical infrastructures in order to improve the manageability of critical infrastructures, particularly in response to alarms and problems.
- Security Assessment of Software-defined Networks: This project focused on building virtualized test beds and conducting security evaluation and penetration testing of software-defined controllers and networks.

7) Patrick Hung, FBIT

Patrick C. K. Hung is a Professor and Director of International Programs at the Faculty of Business and Information Technology at the Ontario Tech University, Canada. He is an Honorary International Chair Professor at National Taipei University of Technology, Taiwan. He is currently working with the College of Technological Innovation at Zayed University on several smart city and cybersecurity research projects in the United Arab Emirates. He is also a Visiting Researcher at the University of São Paulo, Brazil and National Technological University (UTN)-Santa Fe, Argentina. Patrick worked with Boeing Research and Technology at Seattle on aviation services-related research with two U.S. patents on mobile network dynamic workflow system. Before that, he was a Research Scientist with the Commonwealth Scientific and Industrial Research Organization in Australia. He also worked in the software industry in Toronto. He is a founding member of the IEEE Technical Committee on Services Computing, and the IEEE Transactions on Services Computing. He is an editorial board member for the IEEE Transactions on Engineering Management, an associate editor for Electronic Commerce Research and Applications as well as he is coordinating editor of the Information Systems Frontiers. He has a Ph.D. and Master in Computer Science from Hong Kong University of Science and Technology, a Master in Management Sciences from the University of Waterloo, Canada and a Bachelor in Computer Science from the University of New South Wales, Australia. He also chairs the Machine Learning, Robotic and Toy Computing Minitrack and Computing in Companion Robots and Smart Toys Symposium in the Hawaii International Conference on System Sciences (HICSS).

Some of Dr. Hung current project include:

- Gathering Input from Seniors on Legal and Ethical Issues related to Use of Social Robots for In-home Support - SSHRC
- Children Privacy Protection Engine for Smart Anthropomorphic Toys - NSERC
- Test platform for connected and autonomous vehicles and transportation electrification infrastructures (CAVTE) - Canadian Standards Association and NSERC

8) Les Jacob, Vice-President, Research and Innovation

Dr. Jacobs is a leading international expert in applications of data science to research questions involving equality of opportunity, human rights policy, and access to justice; health and human rights in the Asia-Pacific (especially China and Japan); and applied social research methods for large projects involving data science. He was recently the York Research Chair in Human Rights and Access to Justice (Tier 1), where he led the Access to Justice Data Science Lab, as well as Professor and Director of the Institute for Social Research at York University.

Dr. Jacobs' administrative leadership includes serving as Chair of the Senate Academic Planning, Policy Research Committee at York University; the inaugural Director of the York Centre for Public Policy and Law; Executive Director and Senior Research Fellow of the Canadian Forum on Civil Justice; Academic Director of the Statistic Canada Research Data Centre; and Director of the Institute for Social Research.

He has served on numerous public sector research advisory boards and has undertaken public policy research and studies for many organizations including the Law Commission of Canada, Ontario Human Rights Commission, Community Legal Education Ontario, York Region Data Consortium, Ontario Literacy Coalition, Consumer Council of Canada, Windsor Police Service, Industry Canada, International Trade and Labour Program (HRSD Canada), Ottawa Police Service, Office of the Privacy Commissioner of Canada, and Elections Canada. In 2017, he served as Principal Consultant for Cabinet Office for the development of the race data collection

framework for the Government of Ontario and the Broader Public Sector, which was embedded in the new law, The Anti-Racism Act, 2017. He led in 2018 the survey research for the Independent Street Checks Review in Ontario and the review of the Respectful Workplace Policy in the Ontario Public Service for Cabinet Office as well as the expert advisor for Legal Aid Ontario's five-year strategic planning.

Dr. Jacobs held full-time teaching positions at the University of British Columbia and Magdalen College, Oxford University. In 2017 he received the highest honour for a Canadian scholar—Fellow of the Royal Society of Canada, Academy of Social Science—for his internationally recognized contributions in data science to human rights, equality of opportunity, and access to justice.

Dr. Jacobs received his PhD in Politics from Oxford University in the United Kingdom. He also earned his Master of Political Science and Bachelor of Arts (Honours) in Political Science and Philosophy from Western University (London, Ontario).

Some of Dr. Jacobs work include:

- Privacy Rights in the Global Digital Economy: Legal Problems and Canadian Paths to Justice (Irwin Law Books, 2014)

9) Stephen Jackson, FBIT

Stephen Jackson is an Associate Professor in Management Information Systems at the Faculty of Business and Information Technology. Stephen has taught at various universities in the UK, including the University of London, University of Southampton and Queen's University of Belfast. Prior to joining academia, Stephen was an IT consultant for PricewaterhouseCoopers. He has worked on a variety of IT projects across various industry sectors in Europe and Asia. He has published in a number of international journals. His research focuses on behavioral information security and social aspects of implementing and managing computer-based systems.

Some of Stephen's current and past project include:

- The impact of data breach severity on the readability of mandatory data breach notification letters. This project investigated the impact of data breach severity (e.g., total number of breached records, type of data accessed, the source of the data breach and how the data was used) on the readability of data breach notifications from US organizations.
- Self-presentation strategies when responding to data breach**:** looking at self-presentation strategies (reading ease, rhetorical features, thematic factors, use of font styles etc.) used by firms when responding to a data breach. Trying to find out if any self-presentation strategy, or combination of strategies, is particular effective when responding to a data breach.

10) Fletcher Lu, FBIT

Dr. Fletcher Lu is an Associate Professor at Ontario Tech U, with a Ph.D. from the University of Waterloo in Artificial Intelligence and a Master's degree in Scientific Computation. He specializes in Machine Learning Techniques applied to areas of fraud, insurance and health. His collaborations include an industrial post-doctorate with the Canadian Chartered Accountants, contract work with the Communications Security Establishment Canada and an NSERC Collaborative Research and Development grant with Medavie Blue Cross.

Some of Fletcher's current and past project include:

- Auditing for Fraud Risk in Health and Business Insurance with MDPs: This project developed a new algorithm approach for fraud auditing that utilize Markov Decision Processes applied to statistical machine learning and data mining to dynamically uncover patterns of fraud in both business and health areas.
- Network Security with Low-powered devices: The objective of this project is to develop machine learning techniques to detect anomalies in low-powered wireless devices to detect intrusions and illegitimate activities on these networked devices.

11) Stephen Marsh, FBIT

Stephen Marsh is an Associate Professor and computational philosopher with extensive experience in the application of human social norms such as trust, forgiveness and wisdom to computational and information systems. He is the inventor of the concepts of Computational Trust and Device Comfort, and the co-originator of Slow Computing. He works primarily towards the empowerment of people through enabling socio-technical systems to enhance awareness, give advice, and provide encouragement. His work has been applied and published in areas as diverse as social psychology, information systems, HCI, CSCW, AI, Information Security and Mobile Device Awareness.

Prior to being with Ontario Tech University, Steve worked within Canadian Government Laboratories (NRC and CRC) as a research scientist for 16 years, and before that he was a Lecturer in Computing Science at the University of Stirling from 1993-1996. He has been a visiting scholar at the University of Glasgow and Northumbria University in the UK, and a Mercator Fellow at Darmstadt Technical University. He has been an adjunct professor at Carleton University (Systems and Computer Engineering and Cognitive Science) and the University of New Brunswick (Computer Science) as well as Ontario Tech University (Business and Information Technology).

Steve has supervised to successful completion PhD, Masters and Undergraduate projects in areas such as Human Computer Interaction, Trust Management, Intrusion Detection, Device Comfort, Privacy, Information Security and Multi-Agent Systems. He is the author or co-author of numerous conferences, journal, and book chapters and the odd patent. Steve is the Chair of IFIP Working Group 11.11 (Trust Management) and Canadian Delegate to IFIP Technical Committee 11 (Security and Privacy Protection in Information Processing Systems).

Some of Stephen's current and past project include:

- Device Comfort: Device Comfort is both formalization of relationship and user interface design for heightened user awareness of security 'problems' whilst using mobile devices. We developed the Device Comfort paradigm for mobile devices over the past ten years as an extension to the human-device relationship that considers a bi-directional trust relationship between human and mobile device.
- Trust and Information: the project focuses on developing a detailed model of the trustworthiness of information, that is based on journalistic principles combined with a crowd-based and individual trust-history based reasoning on individual information items.
- The Human-AI Trust Relationship: this project examines the trustworthiness of AI as well as the conception of trust in AI for humans. This is a significant divergence from existing AI trustworthiness research in that it considers the bidirectional nature of the phenomenon and acknowledges the need for different trust antecedents in different contexts. It also considers the Media Equation effect, in which people treat technologies as if they were human actors in a system and seeks to understand and model this better for AI-human systems.

- Mobile Privacy enabled through Trust Measures: We developed a model for trust in data handlers that allows mobile device users to determine when health information is shared and to whom, for what purpose, based on a trust matrix derived from a set of simple measures. This is extensible to different forms of information and contexts to allow devices to better protect and compartmentalize information.
- Trust as a User Interface Tool for Computer Security: this project proposed the use of trust to help people determine how to protect their devices and information: interfaces can use simple trust questions related to context and behaviors to determine how best to protect assets and explain this protection in more human-oriented ways.
- Autonomous Information, Privacy and Trust: this project developed a system of information sharing that atomized information and encapsulated it in autonomous agents which could determine with whom to share that information.

12) Qusay Mahmoud, FEAS

Qusay Mahmoud is a Professor of Software Engineering in the Department of Electrical, Computer and Software Engineering. His research interests are in middleware, software systems and security. Dr. Mahmoud joined Ontario Tech University in January 2013 as Professor and Founding Chair of the Department of Electrical, Computer and Software Engineering, and has served in that position until June 2015, followed by one year as Associate Dean (Academic) of the Faculty of Engineering and Applied Science. He moved to Ontario Tech from the University of Guelph where he was a Professor of Computer Science and Director of the Centre for Mobile Education and Research.

Some of Dr. Mahmoud's current project include:

- SidekickVPN: SidekickVPN is an AI-enhanced modern VPN for users who want to be in control of their privacy. It is easy to install, easy to use and cost-effective.

13) Andrea Slane, FSSH

Dr. Andrea Slane is Associate Dean, Research, and Associate Professor in Legal Studies, Faculty of Social Science and Humanities, Ontario Tech University, Oshawa, Ontario Canada. Her research focusses on law's interface with digital communication technologies. She has published on a range of topics at this interface, including on the nature of privacy interests in sexual images; the appropriate limits to privacy protection online; legal approaches to various forms of online and other digital exploitation of vulnerable people; and personality rights and other efforts to use intellectual property to protect personal information and identity.

Some of Dr. Slane's current project include:

- Privacy Protective Lawful Access Technologies: This project I am working on in a collaboration across legal and tech disciplines, including faculty from University of Toronto (Lisa M. Austin – Law; David Lie – Computer Science) and University of Waterloo (Ian Goldberg – Computer Science). We are working on both ends of a data governance framework: the legal end, to establish what the permissible scope is of police access to personal and meta-data in large datasets, and the technical, to devise a tool (or an approach to devising a tool) that would restrict police access to only legally relevant data in a privacy protective way.

- Knowledge Gaps and other Barriers to Cross-sectoral Collaboration in Investigating and Supporting Victims of Online Child Sexual Exploitation Materials: This project is mostly completed, as it was funded by the SSHRC Partnership Development Grant from 2015-2018. The project lead was Jennifer Martin from Ryerson University, Child and Youth Services, and I was co-PI. We held 12 focus groups with members of partner organizations in law enforcement, children's mental health, and child protection. The aim of the project was to discuss knowledge gaps and barriers to collaboration across sectors that deal with investigations and victim support arising from child sexual abuse images.
- Child Pornography; Youth Self-produced Sexual Images; Luring; Revenge Porn

14) Julie Thorpe, FBIT

Dr. Julie Thorpe is an Associate Professor at Ontario Tech University. Prior to that, she had 8 years of experience working in the IT security field. She has served on the program committee for various leading international computer security conferences including ACM CCS, USENIX Security, and ACSAC. Her current research is in human factors and computer security, with a focus on user authentication. Her research has been featured in various media outlets, including Wired magazine, Popular Science, BBC World News, The New York Times, CBS News Sunday Morning Show, CBC Radio's "The Current", Reader's Digest, and the Toronto Star.

Some of Dr. Thorpe current project include:

- Password Semantics. This work investigates the semantic patterns underlying user choice in text passwords. Using 32 million publicly leaked passwords, the research team employed natural language processing techniques and customized visualizations to detect semantic patterns.
- Implicitly Reinforced System-Assigned Passphrases. This work provided the first demonstration that implicit learning can reinforce a user's memory for system-assigned passphrases. We designed and developed a novel passphrase authentication system that employs two implicit learning techniques (contextual cueing and semantic priming), to enhance the memorability of system-assigned passphrases.
- Geographic Authentication. During this project, the research team designed and implemented *GeoPass*, a location-password system, and conducted a multi-session lab/online user study involving 35 participants to evaluate its usability, memorability, and security.
- Presentation Effect. This work aims to make user choices in click-based graphical passwords less predictable through altering a user's perception of a background image during password creation.

15) Christopher O'Connor, FSSH

Dr. Christopher D. O'Connor is an Assistant Professor of Criminology at Ontario Tech University (University of Ontario Institute of Technology). He earned his PhD in Sociology at the University of Calgary in 2010. His research examines resource boomtowns, people's use and perceptions of emerging technology, policing, young people's participation in crime, and school-to-work transitions. Some of his published articles have examined young people's participation in auto theft, people's perceptions of fracking technology, and police use of social media.

Some of Dr. O'Connor's projects include:

- Cyber-attacks on energy infrastructure
- Emerging technology use in policing
- Examining people's perceptions of robots.

16) Miguel Vargas Martin, FBIT

Dr. Miguel V. Martin is a Professor of Computer Science at Ontario Tech University. He has a PhD (Computer Science) from Carleton University, a Master's degree (Electrical Engineering) from CINVESTAV del IPN, and a Bachelor of Science (Computer Science) from UAA. He is a licenced Professional Engineer in the Province of Ontario. His research focuses mainly on computer authentication paradigms and the use of phenomena of the human mind via physiological feedback (e.g., brain-computer interfaces) as well as proven techniques from the psychology field. In the process, he touches upon multi-objective optimization and evolutionary computation. His research over the past decades has relied on machine learning to make sense of large data sets from the real-world. Dormant areas which lost traction for a number of reasons include network steganography in the form of Wi-Fi hidden-channels, adaptive online learning systems, and combating internet child exploitation. Dr. Martin has supervised over 60 graduate and undergraduate students and published his research in over 100 peer-reviewed journals and conferences.

Some of Dr. Martin's current and past project include:

- Privacy-by-design in building Artificial Empathy in anthropomorphic robots. This project aims at removing the need for speech-related Cloud services so that the interaction with robots can be more natural and the human can build trust with the robot.
- Password recall, perceived memorability, and strength using brain-computer interfaces. We use BCIs to read brain signals elicited upon visual stimuli related to passwords, then utilize machine learning techniques to make sense of these signals within the context of password strength and memorability.
- Relationships between passwords and personality. We have found that certain personality types may be correlated to selecting passwords with specific characteristics which could mean that some personality types truly are more vulnerable to password guessing attacks.
- Improving password and passphrase memorability. Here we use proven techniques from psychology and tailor them within the realm of authentication to help users remember their pass codes. For example, we have used contextual cueing and semantic priming to help users remember strong passphrases, resulting in significant memorability improvements.

17) Richard Pazzi

Dr. Richard Pazzi is an Associate Professor at the Faculty of Business and Information Technology, Ontario Tech University, Canada. He received his Ph.D. degree in Computer Science from the University of Ottawa, Canada, in 2008. His research interests include fault-tolerant data dissemination protocols for Wireless Sensor Networks and Mobile Computing. He is also active in the areas of Vehicular Ad Hoc Networks, multimedia communications and networked 3D virtual environments. He is the recipient of Best Research Paper Awards from the IEEE International Conference on Communications (ICC 2009), the International Wireless Communications and Mobile Computing Conference (IWCMC 2009), the IEEE Symposium on Computers and Communications (ISCC 2015), and from the 5th International Conference on Advances in Vehicular Systems, Technologies and Applications (VEHICULAR 2016). He is also

the recipient of Elsevier's Top Cited Article (2005–2010) for his work published in the Journal of Parallel and Distributed Computing (JPDC 2006). He served as co-chair of numerous IEEE and ACM sponsored conferences including ACM DIVANET 2011, ACM Performance Modeling and Monitoring of Heterogeneous Wired and Wireless Networks 2007–2013, and IEEE GLOBECOM 2014 Next Generation Networks Symposium.

Some of Dr. Pazzi's current and past project include:

- Data dissemination in wireless ad hoc networks (vehicular and sensor networks): This project involves the development of novel data dissemination techniques for vehicular networks.
- Context-aware vehicular networks: This project aims at devising innovative solutions that exploit social-network concepts and contextual data around drivers, vehicles, and roads to provide drivers and passenger with intelligent navigation systems.
- Localization and target tracking in vehicular and sensor networks: This project focused on developing efficient localization systems, which is one the technological pillars for ITS applications, and target tracking in both vehicular and sensor networks.
- Multimedia Networks for Emergency Preparedness: This project aims at developing innovative interactive virtual environment streaming mechanisms to be used by applications in emergency preparedness, firefighting, indoors search and rescue, etc.
- Smart Road Sensing Technologies: This project is focused in developing a vehicular detection system and the underlying algorithms with the objective of reducing the costs related to maintenance of smart detection systems for automated traffic light control by replacing existing induction loop traffic systems.

18) Ed Waller, FESNS

Dr. Ed Waller is a Professor at the University of Ontario Institute of Technology (UOIT), in the Faculty of Energy Systems and Nuclear Science, Oshawa, Ontario, Canada. He is currently an Industrial Research Chair in Health Physics and Environmental Safety. Ed earned his BSc in Physics and MScE in Chemical Engineering at the University of New Brunswick (UNB), his Masters in Nuclear Security at Technical University Delft (TUDelft), and his PhD in Nuclear Engineering at Rensselaer Polytechnic Institute, New York (RPI). He worked for over 15 years in industry for Science Applications International Corporation, primarily in threat assessment, health physics and applications of radiation. He is a member of the International Nuclear Security Education Network (INSEN) and former Working Group I (Exchange of Information and Development of Materials for Nuclear Security Education) Chairperson of INSEN. He has been invited to numerous consultancies at the International Atomic Energy Agency (IAEA) for nuclear security document development, and has been Chair of these consultancies. Ed is a Professional Engineer (PEng), Certified Nuclear Security Professional (CNSP), Certified Associate Industrial Hygienist (CAIH) and Certified Health Physicist (CHP). He teaches radiation protection, health physics, environmental effects of radiation, Monte Carlo methods, nuclear security and nuclear forensics at UOIT, and performs research in areas of nuclear security, emergency preparedness and response, radiation dosimetry, applied health physics, radiation safety, and threat assessment.

Some of Dr. Waller's current and past project include:

- Radioactive Source Security Management
- Consideration of Administrative Monetary Penalties in Nuclear Security Regulation
- Physical Design of a Nuclear Facility Security Training Environment and Interfacing with Adversary Probability of Interruption Software

B. Research Facilities

The Faculty of Business and Information Technology boasts a number of world-class research laboratories with infrastructure dedicated to conducting a unique blend of undergraduate and graduate research in a variety of research areas. Of particular relevance to the field of cybersecurity research, these facilities are:

- Hacker Research Laboratory: a cloud-based, networked and isolated lab that houses various networking devices such as servers, firewalls, intrusion prevention/detection systems, and routers. Faculty members use it to conduct various IT security research projects including business process integration, electronic negotiation and agreement, interconnection protocols, mitigation of denial-of-service attacks, network intrusion prevention, detection and reaction, security and privacy, and services computing.
- Information Forensics and Security Laboratory (IFSLab): The IFSLab performs innovative research and development on securing and analyzing networks, computer systems and data. The lab includes space and facilities for students to comfortably perform their research, discuss, collaborate and visualize data.
- Advanced Networking Technology and Security (ANTS) research lab: home to state-of-the-art research and development of technologies for next-generation networks and critical infrastructures. It includes the Canada Foundation for Innovation-funded security testing facility, a private research cloud environment and a software-defined networking testbed
- Networking Laboratory: purpose-built to support the Cisco Networking Academy curriculum, which uses state-of-the-art networking equipment to teach concepts ranging from fundamental networking skills up to enterprise level network engineering.
- Human Machine Laboratory: an interdisciplinary research laboratory devoted to projects at the convergence of human-computer interaction, security and privacy. The lab is focused on building theoretical models and technical systems for securely managing data in 1) brain-computer interfaces for user authentication, and 2) child's play privacy in smart toys.

These research facilities, in addition to numerous other FBIT laboratories, are located in the new SIRC building.