SPONSORSHIP PROSPECTUS

siberX

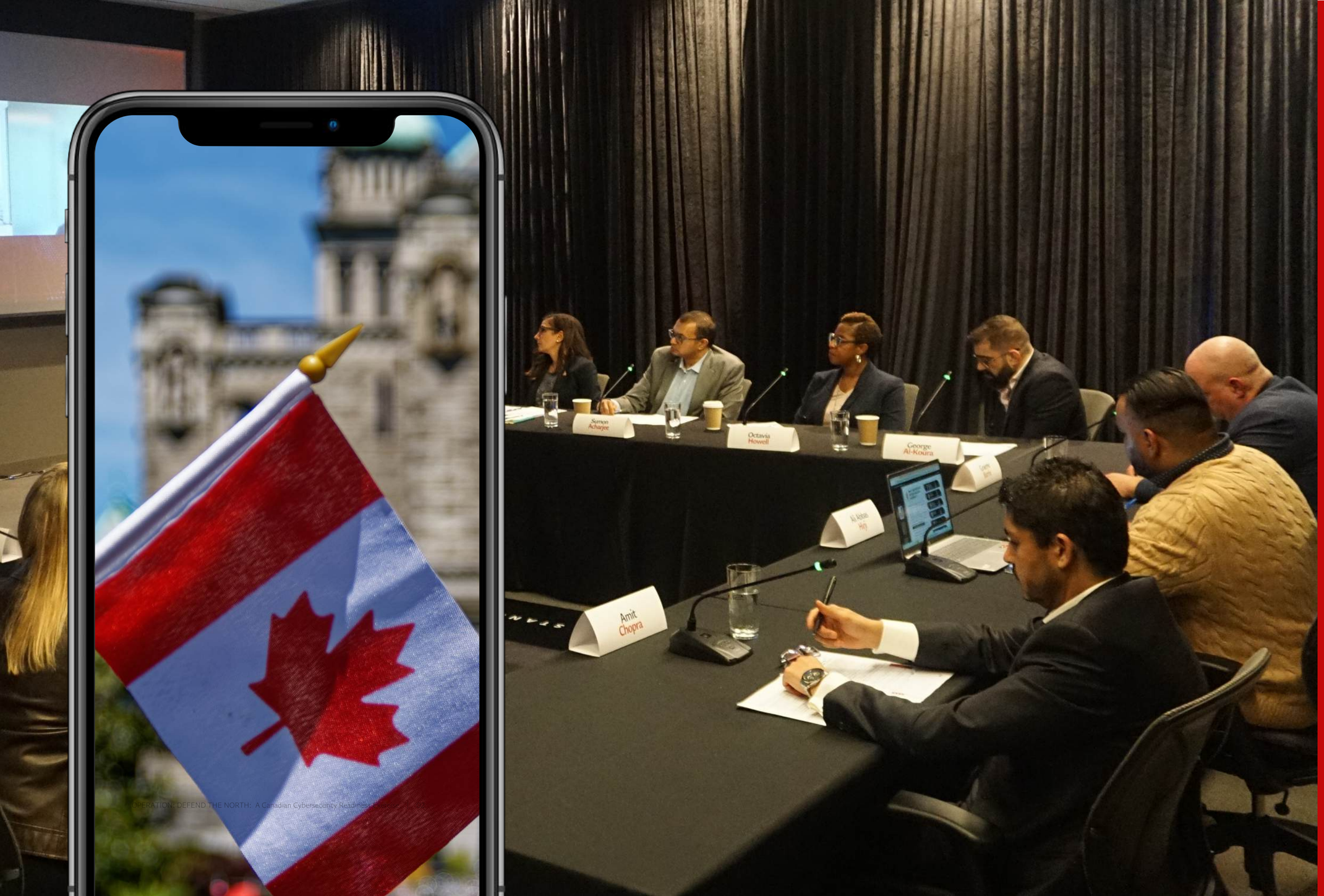
OPERATION: DEFEND THE NORTH

A Canadian Cybersecurity Readiness Exercise

APRIL 3, 2025.

SIMON FRASER UNIVERSITY, VANCOUVER
BRITISH COLUMBIA, CANADA

IN PERSON & DIGITAL



OPERATION: DEFEND THE NORTH

A Canadian Cybersecurity Readiness Exercise

siberX is excited to announce its 3rd cybersecurity readiness table top exercise (TTX). This one day cyber breach simulation event will take place at the beautiful Morris J. Wosk Centre For Dialogue at Simon Fraser University in Vancouver, Canada on April 3rd, 2025 and is designed to strengthen Canada's cybersecurity readiness and response strategies.

This event brings together Public and Private sector stakeholders along with the Canadian Cybersecurity community to discuss how their organizations would respond to such an attack.

Participants, in real-time, will deal with an active incident and breach - collaborating with leaders from across Canada, technical and operational solutions will be proposed to contain the attack.

O Canada, we stand on guard for thee.
Protégera nos foyers et nos droits.

PAST SPONSORS

SentinelOne, Canon, SailPoint, TELUS Business, ARMIS, CDW, aws, CROWDSTRIKE, OBSIDIAN, TANIUM

PAST PARTNERS

CYBER SECURITY CENTRE OF EXCELLENCE, Ontario

siberX

OPERATION: DEFEND THE NORTH

PAST ADVISORY BOARD

Rhonda Bunn
CAO
Town of Midland

Kristi Honey
CAO
Township of Uxbridge

Abdul Karim
CISO
Unity Health Toronto

Octavia Howell
VP, CISO
Equifax Canada Co.

Anshul Srivastava
CISO
TTC

George Al Koura
CISO
RUBY

Bil Harmer
Operating Partner & CISO
Craft Ventures

Cat Coode
Data /Privacy Strategist
Binary Tattoo

Ali Shahidi
Director, Information Security & Risk
TCHC/TSCHC

Jassi Kaur
Director of IT and Security
Bulk Barn

Dr. Eman Hammad
Security & Privacy Working Group Co-Chair
IEEE Future Networks Initiative

Ali Abbas Hirji
CISO
YES

Gemma Ahn
CIO
Brock University

Kush Sharma
Founder
KnightSpectre

Iain Paterson
CISO
WELL Health Technologies

John Pinard
VP, IT Operations, Infrastructure & Cybersecurity
DUCA Financial Services Credit Union

Terry T
Acting Head, Cyber Investigations Unit
CSIS

Tommaso Lorenzo
Manager, Cybersecurity
Niagara Health

Vaughn Hazen
CISO
CN

Bob Gordon
Strategic Advisor
Canadian Cyber Threat Exchange

Vivek Khindria
Former SVP Cyber Security, Network, Technology Risk
Loblaw Companies Limited

Terence Malamtombee
AVP Cyber Strategy. Governance and Control
TD Bank

Emerson Rajaram
CISO
Wellington-Dufferin-Guelph Public Health

Mark Dillon
VP of IT
Enova Power

Kim Schreader
Director, Cybersecurity Professional Services
TELUS Communications

Renee Guttmann-Stark
Founder, CISO
CisoHive

Vivienne Suen
Distinguished Arcitect
TD Bank

Nilesh Shastri
CISO
Canadian Institute of Health Information

Roozbeh Taheri-Nia
Founder
InCloud Security

Dhanush Liyanage
Senior Manager, Cyber Security Defense Operations
Ontario Health

Daniel Pinsky
CSO
CDW Canada

Lina Dabit
Unit Commander Cybercrime Investigative Team
RCMP

Kelley Irwin
Strategic Advisor, Board Director
Descartes Systems Group

Olawumi Alofe-Babalola
Cybersecurity Leader & Advocate
Bank of Canada

Osman Saleem
ICS Cybersecurity Program Manager
GTAA

Shakeel Sagarwala
Chief Information Security Officer
Canadian Tire Bank

Rachel Babins
Founder
Bell

Shilpa Dahiya
Director, Information & Cyber Security
CAAT Pension Plan

Sunil Chand
VP, Security Practice
Centrilogic

Shelley Wark-Martyn
Strategic Training Executive
SANS

Wes Sheppard
CISO
OrderGrid

Amit Chopra
Head of Information Systems
Lakefield College School

Kris E
RCMP

Sherry Rumbolt
Senior Cybersecurity Strategist
Treasury Board of Canada Secretariat

Mirza Baig
Director, Cyber Security
MPAC

Teodor Pana
Director, Cyber Security
SE Health

KEY HIGHLIGHTS

- **Leaders from Critical Sectors Involved in Exercise:** Energy, Financial, Healthcare, Government Services, Telecommunications and Retail.
- **Simulated Cyber Attacks:** Engage in sector-specific cyber threat scenarios
- **Expert-Led Sessions:** Technical and operational discussions with industry leaders - real-time visualizations from an active environment will be incorporated
- **Networking Opportunities:** Connect with professionals across sectors and showcase.

EVENT OVERVIEW:

- **Duration: April 3, 2025.**
- **Format:** Tabletop event held at Simon Fraser University, Vancouver British Columbia, Canada
- 9:00 am - 6:30 pm Exercise and Networking
- **Objective:** Join professionals across sectors working towards protecting a cyber attack against Canada's critical sectors via a cybersecurity readiness exercise

---

DEMOGRAPHICS:

- **PUBLIC/PRIVATE SECTOR:** 50% public & 50% private sector viewing this online, expected attendance, 300 leaders in-person & 3,000+ online.
- **MEDIA:** Media has been invited and will partcipate in coverage (Globe & Mail, Toronto Start, Technology Media)
- **DIGNITARIES:** Minister of Public and Business Service Delivery, CIO & CISO Provinces, MPs Mayors, and Councillors invited to open each day and participate.

MODULE & SPONSORSHIP OPPORTUNITIES

West Coast Dead Zone

It's a typical rainy morning in British Columbia. People are settling into their routines: students head to school and commuters navigate the busy highways and businesses open their doors for the day. Then at precisely 9:15 AM PST, everything changes. Mobile phones lose signal and internet connections drop and landlines fall silent. The province goes eerily quiet as people scramble to understand what's happening.

At first, the outage seems like a technical glitch. Local telecom providers suggest routine maintenance but as the minutes turn to hours, it's clear this is no ordinary disruption. By midday, the outage has affected every corner of the province from bustling Vancouver to remote northern towns. Emergency services are overwhelmed with calls reporting dead communication lines and businesses struggle to process transactions without internet or phone connectivity. Panic rises as families lose contact with loved ones and vital services like 911 dispatch face unprecedented strain.

It's not just BC's citizens affected; key industries reliant on constant communication from healthcare to transportation are in turmoil. Hospitals face delays as internal networks struggle to stay online while airlines operating out of YVR ground flights due to safety concerns. Government officials scramble to reassure the public but the absence of clear information only fuels speculation. Social media becomes a hotbed of conspiracy theories with #BCHack trending nationwide. Emergency broadcasts are limited to old-fashioned radio and long queues form outside gas stations and grocery stores as people stockpile essentials fearing the worst.

By late afternoon, cybersecurity specialists from across Canada are on the ground joined by federal agencies and the RCMP's cybercrime unit. Their challenge is immense: identify the attackers, contain the breach and restore service to millions of desperate residents. Each passing hour raises the stakes as BC's economy grinds to a halt and social unrest begins to simmer. The attack is a wake-up call highlighting just how fragile modern infrastructure can be – and how devastating a single vulnerability can become in the wrong hands.

April 3, 2025 | 9:00 AM - 10:30 AM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 1: **Government Sector** **3 SPOTS REMAINING**	Government officials struggle to maintain order and provide information as panic rises. Law enforcement, alongside federal cybersecurity units, coordinate to investigate the cause of the outage while managing growing public unrest. Misinformation spreads, complicating efforts to reassure citizens - looting is a growing concern as well.	1a. Analysis of the breach 1b. Identifying vulnerable points in the financial network 1c. Coordinating with other banks to share information and strategies 1d. Developing a rapid response plan to restore services 1e. Communicating with the public to manage panic and maintain trust	• CIS Control 1: Inventory and Control of Enterprise Assets • CIS Control 2: Inventory and Control of Software Assets • CIS Control 4: Secure Configuration of Enterprise Assets and Software • CIS Control 12: Implement a Security Awareness and Training Program • CIS Control 13: Email and Web Browser Protections	This module offers sponsorship opportunities for presenting advanced tools and solutions in threat detection and analysis, vulnerability management, and incident response coordination. Along with participating in the live exercise, ideal sponsors would provide cutting-edge cybersecurity solutions specifically tailored for the financial industry. These solutions would enable comprehensive breach analysis, secure information sharing among banks, and rapid response planning to restore services and maintain public trust.

MODULE & SPONSORSHIP OPPORTUNITIES

April 3, 2025 | 11:00 AM - 12:30 PM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 2: **Health** Sector **3 SPOTS REMAINING**	Hospitals and clinics face mounting pressure as internal communication systems falter, delaying critical patient care. Emergency response is strained, forcing healthcare professionals to rely on manual protocols. Backup systems prove insufficient, highlighting vulnerabilities in digital healthcare infrastructure.	2a. Assessing the impact on patient care and prioritizing critical needs 2b. Implementing emergency protocols to manage patient information manually 2c. Coordinating with IT and cybersecurity teams to restore systems 2d. Ensuring the security of sensitive patient data during the breach 2e. Communicating with patients and the public about the situation and ongoing efforts	• CIS Control 3: Data Protection • CIS Control 11: Data Recovery • CIS Control 14: Security Awareness and Skills Training • CIS Control 17: Incident Response Management	This module offers sponsorship opportunities to showcase emergency response solutions, secure patient data management systems, and robust incident recovery tools. In addition to participating in the live exercise, ideal sponsors would deliver state-of-the-art cybersecurity services that ensure the protection of sensitive patient information, support the implementation of manual emergency protocols, and facilitate the rapid restoration of healthcare systems.

April 3, 2025 | 1:30 PM - 3:00 PM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 3: **Utilities** Sector **3 SPOTS REMAINING**	Utility companies grapple with operational challenges. Power and water management teams work to prevent outages while investigating potential cyber threats targeting their networks. Maintenance becomes a manual effort, slowing restoration.	3a. Identifying critical government functions impacted by the attack 3b. Mobilizing emergency response teams to address immediate needs 3c. Coordinating with federal, provincial, and local authorities for a unified response 3d. Ensuring continuity of essential services and public safety 3e. Communicating with citizens to provide updates and guidance	• CIS Control 3: Data Protection • CIS Control 11: Data Recovery • CIS Control 14: Security Awareness and Skills Training • CIS Control 17: Incident Response Management	This module offers sponsorship opportunities to demonstrate comprehensive security solutions for critical government functions, emergency response coordination tools, and continuity planning services. By participating in the live exercise, ideal sponsors would provide specialized cybersecurity products and services that ensure the maintenance of essential services, support a unified response across government levels, and provide clear communication strategies to inform and guide citizens.

MODULE & SPONSORSHIP OPPORTUNITIES

April 3, 2025 | 3:30 PM - 5:00 PM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 4: **Transport** Sector **3 SPOTS REMAINING**	Airports ground flights, ferries halt and public transit is in chaos without reliable communication. Logistics networks break down as deliveries are delayed, and ports face operational paralysis. The industry struggles to adapt, emphasizing the need for resilient contingency plans.	4a. Assessing the impact on transportation networks and supply chains 4b. Implementing contingency plans to maintain critical transport services 4c. Coordinating with transport authorities and logistics companies 4d. Restoring systems and ensuring the security of transport infrastructure 4e. Communicating with the public about delays and alternative arrangements	• CIS Control 7: Continuous Vulnerability Management • CIS Control 17: Incident Response Management • CIS Control 18: Penetration Testing	This module offers sponsorship opportunities to present solutions in transportation network security, supply chain resilience, and system restoration. Along with participating in the live exercise, ideal sponsors would offer advanced cybersecurity measures to protect transport infrastructure, implement contingency plans to maintain critical services, and facilitate effective communication with the public regarding delays and alternative arrangements.

April 3, 2025 | 5:15 PM - 6:15 PM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 5: **Cybersecurity** Sector **3 SPOTS REMAINING**	Cybersecurity specialists lead efforts to identify the source of the attack and restore communication. Coordinated response teams across sectors prioritize essential services to minimize damage. Lessons learned reshape future preparedness and response strategies, underscoring the importance of communication redundancy	5a. Conducting a thorough investigation to trace the origins of the attack 5b. Identifying and closing security gaps in the compromised software 5c. Developing strategies to protect other industries from similar attacks 5d. Coordinating with government and private sector partners for a unified defense 5e. Communicating findings and recommendations to stakeholders and the public	• CIS Control 7: Continuous Vulnerability Management • CIS Control 17: Incident Response Management • CIS Control 18: Penetration Testing	This module offers sponsorship opportunities to showcase advanced threat investigation tools, security gap analysis services, and comprehensive defense strategies. By participating in the live exercise, ideal sponsors would provide state-of-the-art cybersecurity solutions that trace attack origins, identify and close security vulnerabilities, and coordinate unified defense strategies across sectors.

SPONSORSHIP PACKAGE

Showcase your organization, with 1 module, select from the 5 modules **$10,000**

INCLUDED	DESCRIPTION
Booth 8 x 8	A dedicated space at the event for showcasing your organization's offerings, interacting with attendees, and networking with other industry experts.
CASL Compliant List of All Attendees (72 Hours Post Event)	Access to a compliant list of attendees post-event, allowing you to follow up and engage with potential clients or partners.
30-Second Commercial Played During Break/Lunch	A 30-second commercial featuring your organization, played during event breaks or lunch periods to enhance your visibility.
Promotion on Physical Signage, Website, Social Media, and Virtual Platform	Your organization's branding and messaging will be prominently displayed across various event channels including physical signage, the event website, social media platforms, and the virtual event
Session on YouTube	Your module session will be recorded and posted on YouTube, providing ongoing exposure and content for your audience.
3 In-Person Passes & 50 Virtual Passes	3 in-person passes for your team to attend the event physically, and fifty virtual passes for remote participation.
ADDITIONAL	**DESCRIPTION**
Additional Modules	Your sponsorship comes with 1 module, for each additional module the sponsorship price is $5,000
Badge ($3,000)	Sponsorship of event badges, which are worn by all attendees. Your company's logo will be prominently displayed on the badges, providing continuous visibility throughout the event.
Lanyard ($3,000)	Sponsorship of lanyards used to hold attendee badges. Your company's branding will be featured on the lanyards, ensuring that your logo is visible throughout the event.
Breakfast ($2,000) or Lunch ($2,000)	Sponsorship of the breakfast session, providing an opportunity to have your branding featured during the morning meal.
Speakers Lounge ($3,000)	Sponsorship of the lounge area designated for speakers. This exclusive space will prominently feature your company's branding and offer a high-visibility spot to interact with industry leaders.

SPONSORSHIP OPPORTUNITY

Brand Exposure: Position your brand prominently before a diverse audience of industry leaders, cybersecurity professionals, policymakers, and tech enthusiasts via gamified purple teaming.

Thought Leadership: Showcase your expertise through expert-led sessions, workshops, panels, and discussions with industry leaders.

Branding Opportunities: Gain visibility through branding placements across event materials, website, and promotional channels.

Recognition: Acknowledgment as a key sponsor in event communications, press releases, and media coverage.

Community Engagement: Support educational institutions and emergency services personnel by contributing to their practical insights and crisis management skills.

Networking Opportunities: Connect virtually with professionals across sectors, fostering valuable relationships and potential partnerships.

WHO WILL ATTEND?

- **Government Officials:** Responsible for critical infrastructure protection, including policymakers, agencies, and representatives.
- **Cybersecurity Professionals:** Experts seeking sector-specific insights and hands-on experience in strategic cyber defence.
- **Industry Leaders:** Executives and decision-makers invested in safeguarding their respective sector.
- **Private Sector Entities:** Companies offering cybersecurity tools & solutions, to enhance national cyber resilience.
- **Tech Enthusiasts:** Individuals with a passion for technology and interest in addressing cybersecurity challenges through innovation.
- **Educational Institutions:** Students & faculty in cybersecurity programs, gaining practical insights and experience in simulated crisis scenarios.
- **Emergency Services Personnel:** Those responsible for managing crises, ensuring coordination and effective responses in the face of cyber threats.
- **International Cybersecurity Collaborators:** Professionals from allied nations, fostering cross-border cooperation and sharing insights on global cyber threats.
- **Media and Communication Professionals:** Reporters and communicators covering cybersecurity, contributing to public awareness and understanding.
- **General Public:** Engaged citizens interested in understanding the impact of cyber threats on national security and critical infrastructure.


BREAKING
FINANCIAL MARKETS REACT
BREAKING
NEWS
MIRZA BAIG
DIRECTOR, CYBERSECURITY, eInC
MODULE 6A: IMPACTS TO FINANCIAL MARKETS
Want to Host a TTX? Contact us at www.siberX.org or send an email to marketing
Kush Sharma
OPERATION
DEFEND THE NORTH

LEARN HOW TO PARTICIPATE

Visit siberx.org/defendthenorth

SALES@SIBERX.ORG

155 COMMERCE VALLEY DR EAST
THORNHILL, ONTARIO
L3T 7T2