SPONSORSHIP PROSPECTUS

siberX®

OPERATION: DEFEND THE NORTH

A Canadian Cybersecurity Readiness Exercise

DECEMBER 3, 2025.

TORONTO, CANADA

IN PERSON & DIGITAL

OPERATION: DEFEND THE NORTH

A Canadian Cybersecurity Readiness Exercise

siberX is excited to announce its 7th cybersecurity readiness table top exercise (TTX). This one day cyber breach simulation event will take place in Toronto, Canada on December 3, 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.

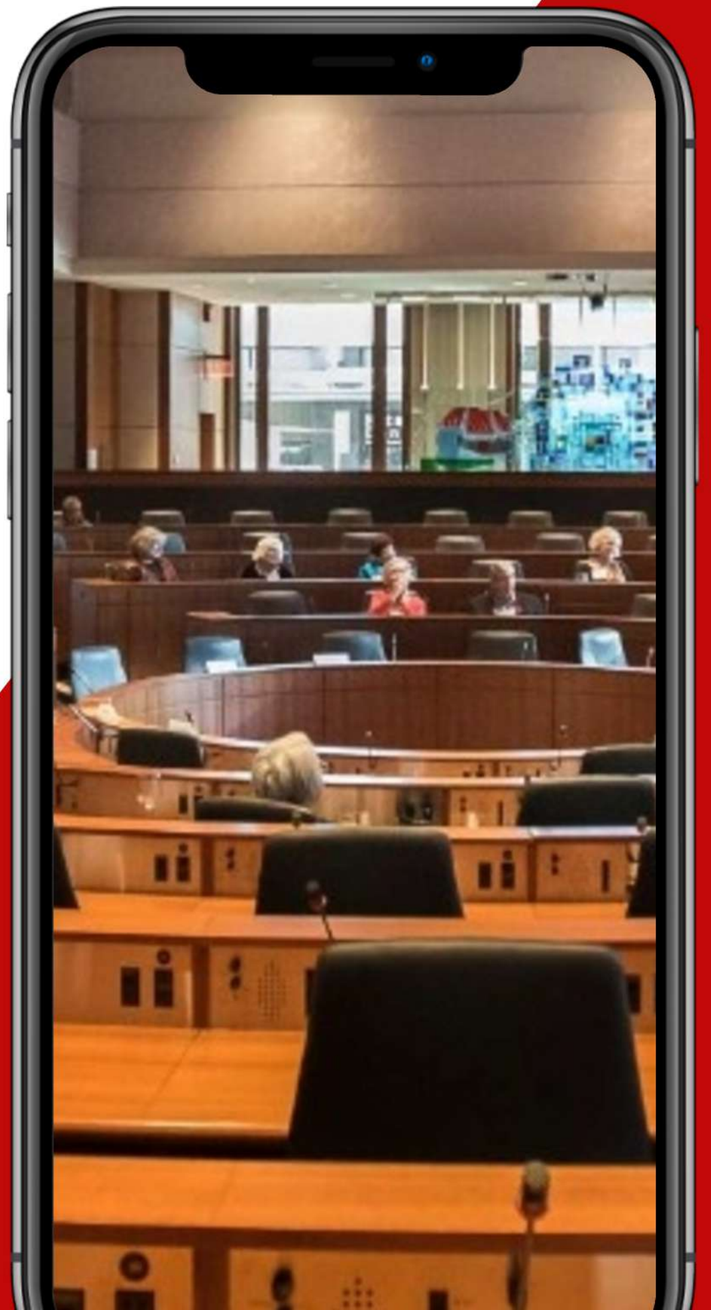
O Canada, we stand on guard for thee.
Protégera nos foyers et nos droits.

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.

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

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

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 for Health Information (CIHI)

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
Co-Founder
ELCH

Shilpa Dahiya
Senior Director, Cybersecurity
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

Anshul Srivastava
CISO
TTC

George Al Koura
CISO
RUBY

Bil Harmer
Operating Partner & CISO
Craft Ventures

Cat Coode
Data /Privacy Strategist
Binary Tattoo

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

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

Terence Malatombee
AVP Cyber Strategy, Governance and Control
TD Bank

Emerson Rajaram
CISO
Wellington-Dufferin-Guelph Public Health

Mark Dillon
VP of IT
Enova Power

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: Dec 3, 2025.**
- **Format:** Cybersecurity Tabletop Event
- 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

Northern Pulse: The Siege on Toronto

Toronto awakens to a sudden wave of disruptions. Subway delays spark confusion. Hospital staff at MapleLeaf Health face locked-out patient records. 911 call centers experience strange interference. Elsewhere, ATMs stop working, mobile banking crashes, and news reports hint at Dominion Banking Group's systems being breached. What at first seem like unrelated technical issues quickly escalate into a coordinated, full-spectrum cyberattack—Operation Northern Pulse.

This is no ordinary disruption. AI-generated deepfakes flood social media with false reports of explosions, political resignations, and foreign interference. TTC riders panic. HydroCore engineers scramble to activate manual controls. The city's digital and physical infrastructure is under siege during a time of high-profile vulnerability—just days before Toronto is set to host a major international tech summit.

The attack reveals its teeth: ransomware locks down critical healthcare and municipal services, zero-click remote code exploits compromise key networks, and suspected supply chain vulnerabilities ripple across sectors. Dominion Banking Group, at the heart of Canada's economy, teeters on the edge of collapse as financial regulators initiate emergency liquidity measures.

As systems are quarantined and countermeasures deployed, a parallel information war plays out—driven by deepfakes, drones, and digital manipulation. A failed physical intrusion at a secure data facility confirms the hybrid nature of the threat. The adversary's goals are clear: destabilize Toronto's economy, fracture public trust, and embarrass Canada on the world stage.

What follows is a tense effort to regain control. Inter-agency coordination is tested as every sector mobilizes. From decryption and patching, to public reassurance and AI-driven counter-messaging, the city fights to restore order. Once the crisis subsides, leaders from across government, industry, and finance gather for a full-scale hotwash—determined to extract lessons, close vulnerabilities, and prevent a repeat.

Dec 3, 2025 | 9:00 AM - 10:30 AM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 1: **Detection and Analysis** **3 SPOTS REMAINING**	Toronto faces a multi-pronged cyberattack: TTC, HydroCore, and city hotlines show issues. "MapleLeaf Health" hospital's patient system is encrypted, and 911 experiences interference. ATMs and online banking fail city-wide, signaling a siege on Dominion Banking Group. AI-generated deepfakes spread misinformation. This is "Operation Northern Pulse," a sophisticated attack targeting Toronto's infrastructure and economy, possibly linked to an international tech summit. The immediate challenge: identify root causes and connections.	1a. Initial Threat Investigation & Breach Analysis 1b. Identifying Vulnerabilities in Telecom Infrastructure 1c. Establishing Secure Communication & Intelligence Sharing 1d. Developing a Rapid Response Strategy 1e.Public Communication & Crisis Management	• CIS Control 1: Inventory and Control of Enterprise Assets • CIS Control 2: Inventory and Control of Software Assets • CIS Control 8: Audit Log Management • CIS Control 14: Security Awareness and Skills Training • CIS Control 17: Incident Response Management	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

Dec 3, 2025 | 11:00 AM - 12:30 PM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 2: **Containment & Discovery** **3 SPOTS REMAINING**	"Operation Northern Pulse" containment halts ransomware and zero-click RCE across city and Dominion networks. HydroCore and TTC enact backups; affected segments quarantined; financial regulators activate liquidity measures. Teams investigate breaches, AI deepfakes, and drone threats to understand the attacker's goals.	2a. Immediate Isolation of Affected Systems 2b. Securing Critical Services and Backup Networks 2c. Identifying Potential Threats and Vulnerabilities 2d. Coordinating Incident Response and Risk Mitigation 2e. Communicating with Key Stakeholders and the Public	• CIS Control 3: Data Protection • CIS Control 4: Secure Configuration of Enterprise Assets and Software • CIS Control 7: Continuous Vulnerability Management • CIS Control 12: Network Infrastructure Management	This module offers sponsorship opportunities for presenting advanced containment, threat isolation, and risk mitigation solutions during a cyber crisis. Ideal sponsors will provide cutting-edge tools for real-time threat detection, automated vulnerability assessment, and critical infrastructure security to ensure telecom networks remain resilient. Along with participating in the live exercise, sponsors will showcase innovative response technologies that enable rapid threat neutralization, secure backup communications, and operational continuity during outages.

Dec 3, 2025| 1:30 PM - 3:00 PM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 3: **Eradication** **3 SPOTS REMAINING**	With root causes found, "Operation Northern Pulse" focuses on removing threats from city systems and Dominion Banking Group. Ransomware is decrypted or rebuilt, patches applied, and zero-click RCE vulnerabilities patched. Counter-drone measures deploy, AI deepfakes are countered with trusted messaging, and a physical breach at DataVault Secure is addressed. Collaboration with CloudNexus Solutions tackles the supply chain compromise. Full threat removal is critical amid the tech summit and economic impact.	3a. Isolating and Neutralizing Active Threats 3b. Identifying and Patching Vulnerabilities 3c. Removing Malicious Network Activity 3d. Verifying System Integrity 3e. Implementing Temporary Security Safeguards During Cleanup	• CIS Control 5: Account Management • CIS Control 6: Access Control Management • CIS Control 10: Malware Defences • CIS Control 15: Service Provider Management	This module offers sponsorship opportunities for presenting advanced solutions in threat removal, malware eradication, and secure system restoration. Ideal sponsors will provide cutting-edge tools for forensic analysis, endpoint protection, and vulnerability patching to eliminate persistent threats and restore telecom operations. Along with participating in the live exercise, sponsors will showcase innovative technologies for automated malware detection, network hardening, and secure infrastructure recovery.

MODULE & SPONSORSHIP OPPORTUNITIES

Dec 3, 2025 | 3:30 PM - 5:00 PM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 4: **Response and Post Incident Activity** **3 SPOTS REMAINING**	Response efforts expand to focus on clear communication with stakeholders, managing public panic, and coordinating with law enforcement and regulators. Recovery prioritizes restoring key city services and Dominion Banking's core functions to ensure safety and stability. Post-incident work includes thorough documentation, evidence preservation, and lessons learned to improve coordination, threat intelligence, and countering information warfare.	4a. Immediate Response and Emergency Coordination 4b. Securing Access to Critical Systems & Controlling Damage 4c. Restoring Public and Enterprise Connectivity 4d. Incident Review and Root Cause Analysis 4e. Strengthening Future Resilience & Cybersecurity Improvements	• CIS Control 7: Continuous Vulnerability Management • CIS Control 17: Incident Response Management • CIS Control 18: Penetration Testing	This module offers sponsorship opportunities for presenting comprehensive incident response, disaster recovery, and crisis management solutions. Ideal sponsors will provide cutting-edge tools for secure communications, breach response coordination, and business continuity planning to minimize downtime and restore public confidence. Along with participating in the live exercise, sponsors will showcase innovative solutions for incident tracking, real-time system monitoring, and cyber resilience enhancement.

Dec 3, 2025 | 5:15 PM - 6:15 PM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 5: **Closing Remarks and Hotwash** **3 SPOTS REMAINING**	As systems recover, a multi-agency hotwash reviews the "Operation Northern Pulse" response. Leaders discuss successes—like quick emergency actions and collaboration—and areas to improve, such as early detection, communication, and public trust. The goal: strengthen Toronto's preparedness, security, incident response, and financial resilience against future hybrid threats.	5a. Finalizing Full Operational Restoration 5b. Reviewing Incident Response & Performance Assessment 5c. Addressing Public Trust & Communication Strategy 5d. Implementing Lessons Learned & Future Resilience Planning 5e. Formal Closure and Leadership Remarks	• CIS Control 7: Continuous Vulnerability Management • CIS Control 17: Incident Response Management • CIS Control 18: Penetration Testing	This module offers sponsorship opportunities for presenting strategic insights, post-incident analysis tools, and long-term resilience planning solutions. Ideal sponsors will provide cutting-edge platforms for forensic reporting, compliance management, and cybersecurity training to strengthen future incident preparedness. Along with participating in the live exercise, sponsors will showcase innovative approaches for lessons learned analysis, policy refinement, and cross-sector collaboration to prevent future crises.

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.


National Economic Impact
$ 120,008,800.40
Time Since Breach 4h 18m 37s
MODULE 3
GOVERNMENT SECTOR
OPERATION:
DEFEND THE NORTH
sberX
MODULE 2
HEALTHCARE SECTOR
MODULE 1
FINANCE SECTOR
MODULE 3
GOVERNMENT SECTOR

LEARN HOW TO PARTICIPATE

Visit siberx.org/defendthenorth

SALES@SIBERX.ORG

155 COMMERCE VALLEY DR EAST
THORNHILL, ONTARIO
L3T 7T2