SPONSORSHIP PROSPECTUS

siberX®

OPERATION: DEFEND THE NORTH

A Canadian Cybersecurity Readiness Exercise

OCTOBER 20, 2025.

CALGARY, CANADA

IN PERSON & DIGITAL

MODULE 3
GOVERNMENT
OPERATION: DEFEND THE NORTH
siberX
Alexander MacLean
Industry Expert
Rhonda Bunn
Councillor

OPERATION: DEFEND THE NORTH

A Canadian Cybersecurity Readiness Exercise

siberX is excited to announce its 5th cybersecurity readiness table top exercise (TTX). This one day cyber breach simulation event will take place in Calgary, Canada on October 20, 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

Mary Carmichael
President
ISACA Vancouver

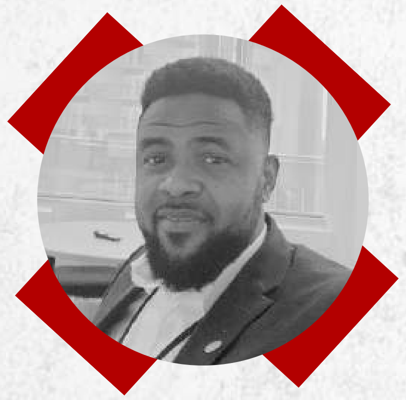
Richard Henderson
Executive Director & CISO
Alberta Health Services

Jillian Carruthers
Assistant Deputy Minister & CTO
BC Public Service

Ali Abbas Hirji
VP Technology and Cyber
Computek College and 369 Global

Octavia Howell
VP, CISO
Equifax Canada Co.

Julia Le
Senior Manager
Ontario Public Service



TJ Odugbesan
Director of Enterprise Security
SaskEnergy

Sherry Rumbolt
Senior Cybersecurity Strategist
Treasury Board of Canada Secretariat

Hardeep Mehrotara
VP Information Security & Architecture
Concert Properties

Vivienne Suen
Distinguished Architect
TD Bank

Parul Kharub
Cyber Security and Tech Risk, Advisor and Business Partner
Teck Resources Limited

Rob Davidson
AVP, CISO
PBC Solutions

Maleena Singh
Director of Incident Response
Mirai Security Inc.

Michael Buckley
Security Operations Center Lead
Mark Anthony Group

Mark Dillon
VP of IT
Enova Power

Neumann Lim
Manager of Cybersecurity
Odlum Brown

Alex Dow
Chief Innovations Officer
Mirai Security

PAST ADVISORY BOARD

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: October 20, 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

West Coast Dead Zone

It's a typical rainy morning in Calgary. 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 Alberta’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 #ABHack 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 AB’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.

October 20, 2025 | 9:00 AM - 10:30 AM				
MODULE	**MODULE DESCRIPTION**	**MODULE BREAKDOWN**	**CIS CONTROL**	**SPONSORSHIP OPPORTUNITY**
MODULE 1: **Detection and Analysis** **3 SPOTS REMAINING**	The collapse of telecom systems sparks widespread disruption, public uncertainty, and a surge of misinformation. This module examines the initial investigation into potential threats, identifying vulnerabilities, and establishing secure communication pathways to analyze and mitigate the impact on critical operations.	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

October 20, 2025 | 11:00 AM - 12:30 PM

MODULE	MODULE DESCRIPTION	MODULE BREAKDOWN	CIS CONTROL	SPONSORSHIP OPPORTUNITY
MODULE 2: Containment & Discovery 3 SPOTS REMAINING	Lives are at risk as vital services lose access to critical communication networks. This module focuses on isolating vulnerabilities, uncovering potential risks, and securing essential systems to ensure continuity of care and operations during the outage.	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.

October 20, 2025 | 1:30 PM - 3:00 PM

MODULE	MODULE DESCRIPTION	MODULE BREAKDOWN	CIS CONTROL	SPONSORSHIP OPPORTUNITY
MODULE 3: Eradication 3 SPOTS REMAINING	The telecoms outage brings key operations to a standstill, disrupting supply chains and critical systems. This module focuses on eliminating threats, restoring functionality, and minimizing economic impact with attempts to reestablish secure and reliable connectivity across essential networks.	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

October 20, 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	Communication blackouts leave communities vulnerable and disrupt essential activities. This module emphasizes responding to breaches, securing access to critical systems, and maintaining operational continuity, while laying the groundwork for post-incident analysis and future resilience.	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.

October 20, 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 telecom networks begin to come back online, how do we restore operations and rebuild trust? This session explores the recovery phase, offering insights into maintaining data integrity, strengthening resilience, and ensuring cross-sector collaboration for future incidents.	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

```
Dec  3 13:20:46 filedrop systemd[1078]: Reached target Exit the Session.
Dec  3 13:22:02 filedrop systemd[1]: Started Session 6 of User ubuntu.
Dec  3 13:22:19 filedrop systemd[1]: Started Session 8 of User ubuntu.
Dec  3 13:22:23 filedrop systemd[1]: Started Session 9 of User root.
Dec  3 13:22:30 filedrop systemd[1173]: Finished Exit the Session.
Dec  3 13:22:30 filedrop systemd[1173]: Reached target Exit the Session.
Dec  3 13:22:40 filedrop systemd[1366]: Finished Exit the Session.
Dec  3 13:22:40 filedrop systemd[1366]: Reached target Exit the Session.
Dec  3 13:22:46 filedrop systemd[1]: Started Session 11 of User ubuntu.
Dec  3 17:50:33 filedrop systemd[1]: Started Session 17 of User root.
Dec  3 17:50:34 filedrop systemd[1434]: Finished Exit the Session.
Dec  3 17:50:34 filedrop systemd[1434]: Reached target Exit the Session.
Dec  3 17:50:35 filedrop systemd[1]: Started Session 19 of User root.
Dec  3 17:50:37 filedrop systemd[1]: Started Session 20 of User root.
Dec  3 17:50:39 filedrop systemd[1]: Started Session 21 of User root.
Dec  3 17:50:40 filedrop systemd[1]: Started Session 22 of User root.
Dec  3 17:50:43 filedrop systemd[1]: Started Session 23 of User ubuntu.
Dec  3 17:50:51 filedrop systemd[1661]: Finished Exit the Session.
Dec  3 17:50:51 filedrop systemd[1661]: Reached target Exit the Session.
ubuntu@filedrop: $
```

LEARN HOW TO PARTICIPATE

Visit siberx.org/defendthenorth

SALES@SIBERX.ORG

155 COMMERCE VALLEY DR EAST
THORNHILL, ONTARIO
L3T 7T2