SPONSORSHIP PROSPECTUS

siberX

OPERATION: DEFEND THE NORTH

Winter Supply Chain Collapse

A Canadian Cybersecurity Readiness Exercise

DEC 3, 2024

TORONTO, ONTARIO, CANADA
IN-PERSON & VIRTUAL

WHATS INSIDE:

OPERATION: DEFEND THE NORTH

A Canadian Cybersecurity Readiness Exercise

siberX is excited to announce its 2nd cybersecurity readiness table top exercise (TTX). This one day cyber breach simulation event will take place in Toronto, Ontario, Canada, on December 3, 2024 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 will collaborate closely to contain and minimize the impact of the simulated attack, showcasing their strategies for recovery and response.

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

PAST SPONSORS

ARMIS CDW aws SailPoint CROWDSTRIKE OBSIDIAN

PAST PARTNERS

CYBER SECURITY CENTRE OF EXCELLENCE Ontario

PAST ADVISORY BOARD

Rhonda Bunn
Chief Administrative Officer
Town of Midland

Kristi Honey
Chief Administrative Officer
Township of Uxbridge

Greg Moshonas
Director, Cyber Security Defense
Ontario Health

Ali Dehghantanha
Canada Research Chair in Cybersecurity and Threat Intelligence
Cyber Science Lab, University of Guelph

George Al Koura
CISO
RUBY

Julia Le
Senior Manager
Government of Ontario

Sherifat Akinwonmi
BISO
TD Bank

Jack Brooks
Head of Hackbusters
BOXX Insurance

Jassi Kaur
Head of IT & Security
Bulk Barn Foods Limited

Ali Shahidi
Chief Cyber Security & Technology Officer
InfoTransec Inc.

Lindsay MacDonald
IT Security Manager, GRC
Cooke Inc.

Rachel Babins
Co-Founder
ELCH

Alpha Chan
CISO
Toronto Police Service

Kush Sharma
Director
MISA Ontario

Graeme Barrie
President
Netmechanics

Martin Stefanczyk
Manager, Office of Project Management and Business Transformation
Town of Aurora

Sumon Acharjee
Chief Information Officer
City of Markham

Octavia Howell
VP, Chief Information Security Officer
Equifax Canada Co.

Vivienne Suen
Distinguished Full Stack Architect
TD Bank

Daniel Pinsky
CSO
CDW Canada

Lina Dabit
Inspector Officer in Charge Federal Policing Cybercrime Toronto
RCMP

Kelley Irwin
Strategic Advisor & Corporate Board Director
Descartes Systems Group

Anshul Srivastava
CISO
TTC

Kajeevan Rajanayagam
Director of Cybersecurity
UHN

Randy Haug
Senior Vice President, Technology & ITSM
CAAT Pension Plan

Amit Chopra
Head of Information Systems
Lakefield College School

Osman Saleem
ICS Cybersecurity Program Manager
Greater Toronto Airports Authority

Dan Elliott
Principal, Cyber Security Risk Advisory
Zurich Resilience Solutions Canada

Mirza Baig
Director, Cybersecurity
MPAC

Nicholas Aleks
Chief Hacking Officer
ASEC

Roozbeh Taheri-Nia
Director, IAM Program
CPP Investments

Sunil Chand
CSO, CISO, board Advisor, Cybersecurity Executive

Arnold Villeneuve
Director
Achieva Tech Incorporated

KEY HIGHLIGHTS

- **Critical Sectors Involved in Exercise:** Energy, Financial, Healthcare, Government Services, Telecommunications, Retail.
- **Simulated Cyber Attacks:** Engage in sector-specific cyber threat scenarios via Modules.
- **Expert-Led Sessions:** Workshops, panels, and discussions with industry leaders.
- **Networking Opportunities:** Connect with professionals across sectors and showcase.

EVENT OVERVIEW:

- **Duration:** December 3, 2024
- **Format:** Tabletop event held in Toronto, Canada.
  - 9:00 am - 5:00 pm Exercise.
- **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 Province Ontario, MPs Mayors, and Councillors invited to open each day and participate.

MODULE & SPONSORSHIP OPPORTUNITIES

Winter Supply Chain Collapse

It's a busy holiday season in Toronto. Shoppers flood malls, gift stores and online platforms, eager to finalize their holiday purchases. The city is alive with festive cheer as residents prepare for the upcoming Christmas celebrations.

Suddenly, confusion spreads - At 10:00 AM EST, reports of widespread payment failures emerge. Initially dismissed as glitches, it quickly becomes apparent that something far more sinister is at play. Debit and credit card transactions fail across the board. ATMs refuse to dispense cash and online banking systems are inaccessible!

Panic sets in as the disruption escalates. News channels and social media explode with reports. The entire country is affected. The problem is traced back to a central operating software used ubiquitously across Canadian industries.

This software, vital for financial transactions, healthcare systems and various critical infrastructures, has inexplicably crashed. Nearly 80 to 90 percent of industries in Canada rely on it, and its sudden failure has brought the nation to a standstill. Hospitals struggle to access patient records and pharmacies cannot process prescriptions. Retailers face chaos as their point-of-sale systems collapse, leading to long queues and frustrated customers.

Experts quickly realize this is a sophisticated supply chain cyber attack. The software, seemingly benign and integral to countless systems, has been compromised. The attackers have struck at the heart of the nation's infrastructure, demonstrating a chilling level of precision and coordination.

Government agencies, cybersecurity firms and industry leaders must now work together to unravel the attack, mitigate the damage and restore normalcy. The stakes are high, and the clock is ticking as the country faces one of its most formidable cyber threats just days before Christmas. The challenge is not just to resolve the immediate crisis but to understand the broader implications and prevent future vulnerabilities.

Each Module will be delivered in 90 minutes. Some modules will assign you specific industry roles to play while others will be a more general discussion. Each module will include one which is technical and furthers the information about the nature of the attack.

Dec 3, 2024 | 9:00 AM - 10:30 AM

MODULE	MODULE DESCRIPTION	MODULE BREAKDOWN	CIS CONTROL	SPONSORSHIP OPPORTUNITY
MODULE 1: **Finance** Sector 3 SPOTS REMAINING	A local bank is the first to report on the attack, prompting an immediate investigation into the root cause. In this scenario, you will join leaders from Canada's financial sector who will be reviewing the technical details of the attack and determining next steps.	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

Dec 3, 2024 | 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 across Canada are struggling as their systems go down, unable to access patient records or process prescriptions. In this scenario, healthcare leaders must collaborate to address the crisis.	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.

Dec 3, 2024 | 1:30 PM - 3:00 PM

MODULE	MODULE DESCRIPTION	MODULE BREAKDOWN	CIS CONTROL	SPONSORSHIP OPPORTUNITY
MODULE 3: **Government** Sector 3 SPOTS REMAINING	Government agencies are hit hard by the software failure, disrupting everything from social services to administrative functions. Leaders must act swiftly to maintain essential services and public order.	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

Dec 3, 2024 | 3:30 PM - 5:00 PM

MODULE	MODULE DESCRIPTION	MODULE BREAKDOWN	CIS CONTROL	SPONSORSHIP OPPORTUNITY
MODULE 4: **Transport** Sector 3 SPOTS REMAINING	The transport industry faces chaos as logistics systems fail, affecting everything from public transit to shipping and delivery services. Industry leaders must navigate the crisis to keep goods and people moving.	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.

Dec 3, 2024 | 5:15 PM - 6:15 PM

MODULE	MODULE DESCRIPTION	MODULE BREAKDOWN	CIS CONTROL	SPONSORSHIP OPPORTUNITY
MODULE 5: **Cybersecurity** Sector 3 SPOTS REMAINING	Cybersecurity experts are at the forefront of the response, tasked with identifying the source of the attack and preventing further damage. In this scenario, you will join top cybersecurity minds working to resolve the crisis.	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 NEWS
FINANCIAL MARKETS REACT
#DEFENDTHENORTH
ATTACK ATTRIBUTED TO CYBERSECURITY ATTACK
NATIONWIDE BLACKOUT SPARKS FEAR AND OUTR
Rachel Babins
Kush Sharma
National Economic Impact
$ 902,750,646.70
Time Since Breach
BREAKING NEWS
#DEFENDTHENORTH
MIRZA BAIG
DIRECTOR, CYBERSECURITY, MPAC
MODULE 4A: IMPACTS TO FINANCIAL MARKETS
siberX Operation Defend The North.
Want to Host a TTX? Contact us at www.siberX.org or send an email to marketing
EXIT SORTIE
OPERATION DEFEND THE NORTH
WE STAND ON GUARD FOR THEE

LEARN HOW TO PARTICIPATE

Visit siberx.org/defendthenorth

SALES@SIBERX.ORG

155 COMMERCE VALLEY DR EAST
THORNHILL, ONTARIO
L3T 7T2