Welcome to February Breakfast

SARIMS
Southern Alberta Risk & Insurance Management Society

@SOUTHERNALBERTARIMS

Sat Parhar

Jeannine Adams

Thank You to Our Sponsors

Platinum

AIG

AON

Gallagher Energy Risk Services

BHSI
BERKSHIRE HATHAWAY SPECIALTY INSURANCE

Gold

Liberty Mutual INSURANCE

SOMPO

prl insurance brokers & advisors

Marsh

ZURICH

Silver

CHUBB

W
A McLarens Company

IRIDIUM
RISK SERVICES EVOLVED

NAVACORD

AI in the Crosshairs: Risks, Resilience, and Leadership in Cybersecurity

AI's Role in Cyber Threats, Risk and Law Enforcement Response

s01ve
Cyber Solutions

Sat Parhar

Jeannine Adams

s01ve.io

A little about s01ve Cyber Solutions

Canadian cybersecurity service provider.

Focuses on prevention.

Former Law enforcement, Insurance & Risk cybersecurity specialists.

Partners with small and medium businesses.

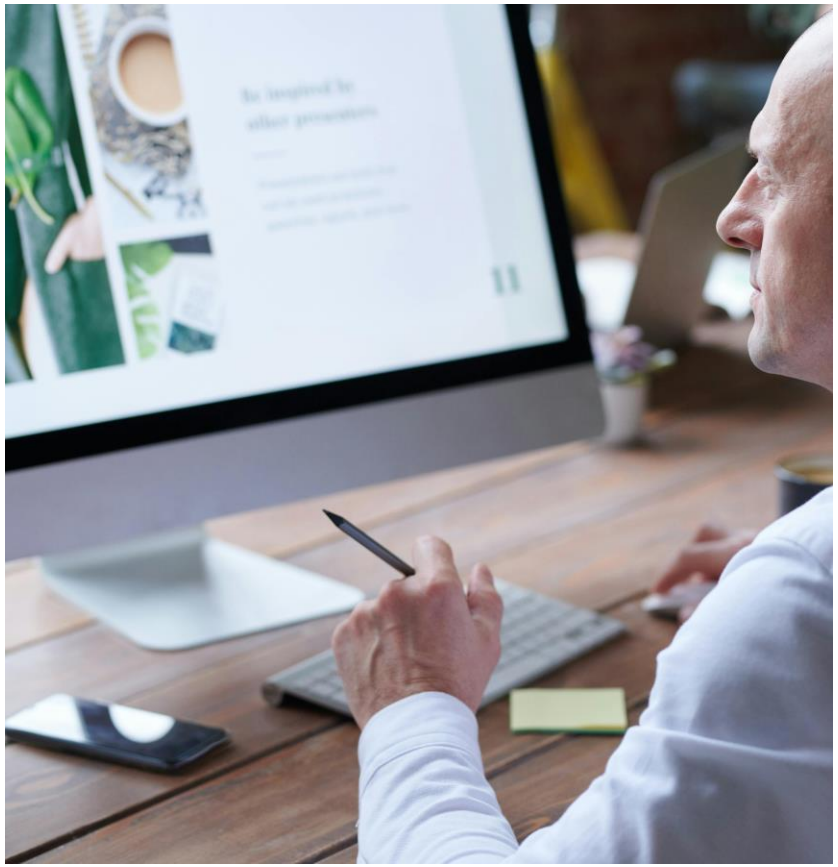
Collaborates with insurance and legal partners.

Cyber Crime Individualized View

- Globally $9.5 Trillion USD in losses (2024)
- Canada 41,000 reported cyber crimes
  - Represents 10-25% of actual incidents.

Let's personalize this:

- Data reveals that **31%** of data breaches led to job losses.
- Of those job losses, **29% were outside the IT department.**
- Cybercrime affects **1 person every 22 seconds** globally.
- Cybercrime in Calgary Out of Control: up 50% from 2023
  - 54% increase in ransomware attacks 50% increase in reported crypto losses 42.8 million
- **Romance scam** victims lose on average **$4,300 CAD** (2023).
- Average phishing click rate is **17.8% & targeted (Spear) at 53.2%.**
- **30% of phishing victims** report being targeted multiple times.



AI Introduction

Manipulative AI-driven cyberattacks

Growing AI accessibility gaps

AI as both an offensive and defensive tool

AI’s Dual Role:

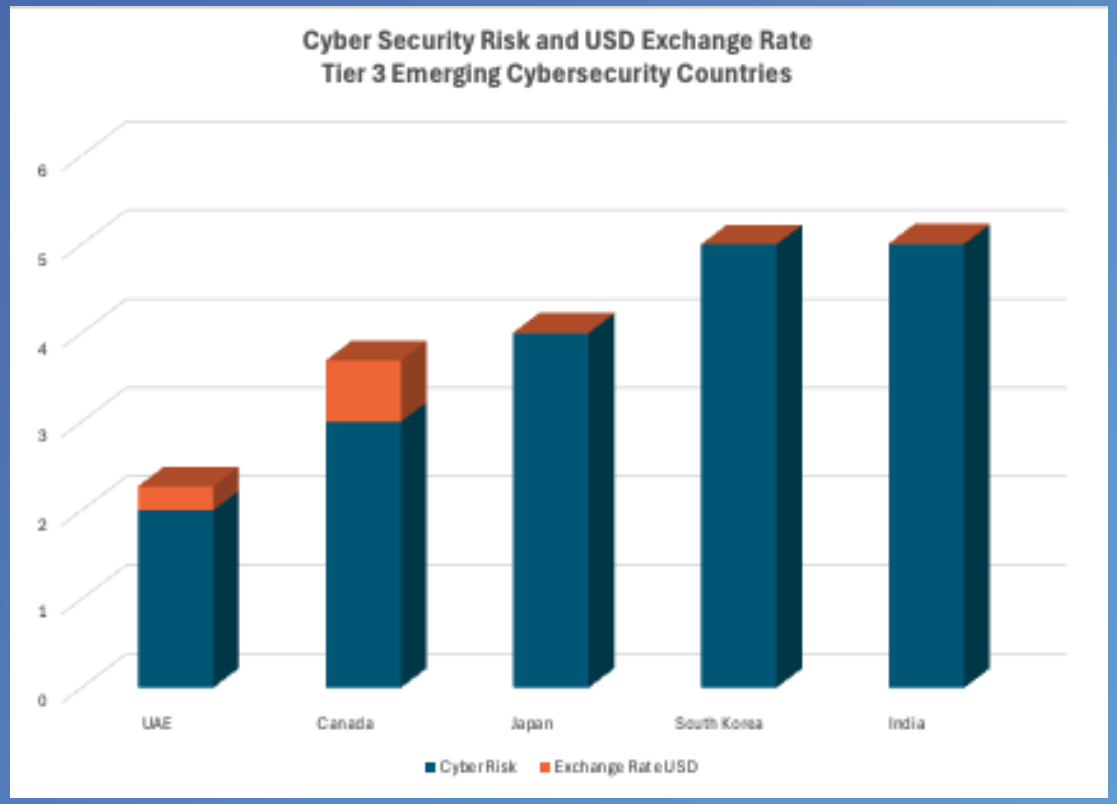
How AI Enables and Defends Against Cyber Crime

AI as Hacking Tool:

- **Deepfake phishing attacks**
- **AI-generated social engineering tactics**
- **AI-automated Exploitations**
- **Personalize Spear-phishing At scale**
- **Adapting in real time to counter law enforcement measures**
- **Malware with Built-in anti-detection**
- **Polymorphic malware**
- **Further lowers technical skills required**
- **Mimic legitimate user behaviour**

AI as a Defense:

- **AI-driven anomaly detection**
- **Automated threat intelligence**
- **AI-assisted security automation**
- **Automated active threat mitigation**
- **Behaviour analysis**
- **Self-healing security systems**
- **AI-Driven Honey pots**
- **AI-Dark Web Monitoring**
- **AI-Table Top Exercises**



Canada's Global Cyber Rank and Impact Indicators

Ranking of Canada: Tier 3 "Emerging Cybersecurity" alongside Japan, South Korea, and India.

- Identity theft, scams and Fraud and ransomware are impacting a larger proportion of businesses
- Identity theft is the largest growth for businesses risk
- Scams and fraud remain the largest portion of method
- Spending on recovery from cyber incidents doubles aka- recovery becoming more severe.

Tier 1: US, UK, Isreal, Singapore, Estonia

Tier 2: EU, Germany, Australia, France

Tier 4: Brazil, Mexico, Nigeria, Iran

Impact of AI on Cyber-Security

Key Indicators

- Increased Sophistication of attacks, increased complexity
  - Deep fakes
  - Social engineering
- Threat actors are investing more time to slightly fewer companies for higher returns
- Increase in AI-Powered Cybercrime
- Generative AI enables highly personalized emails increasing Business Email Compromise
- Lack of AI expertise in companies or law enforcement
- No Canadian Governance at the Federal Government level
- Increased Risk to small and medium businesses as they don’t have processes or education in place

AI Challenges for Law Enforcement

- Limited AI Expertise
- Criminals use AI to generate fake evidence and mislead investigations
- Jurisdictional challenges: Global, Too small, Too Big
- Differential outcomes: active crime vs conviction driven
- Manual investigations vs automated attacks: Speed to respond
- AI Attacks can self modify in real time
- Hackers us AI to disguise their activities

AI and Corporate Risk

Leadership Accountability

- Understand how decisions impact where applied governance resides
- Who decides cyber expectations for clients & vendors (Board, CIO, Risk Officers, IT Manager) should be deciding how to treat clients and vendors when it comes to cyber expectations

Board-level AI oversight

- Understand Personal legal accountability
- Educate them on their own vulnerabilities

Legal and regulatory gaps in AI governance

- Governments are too slow to adapt creating cyber phishing holes

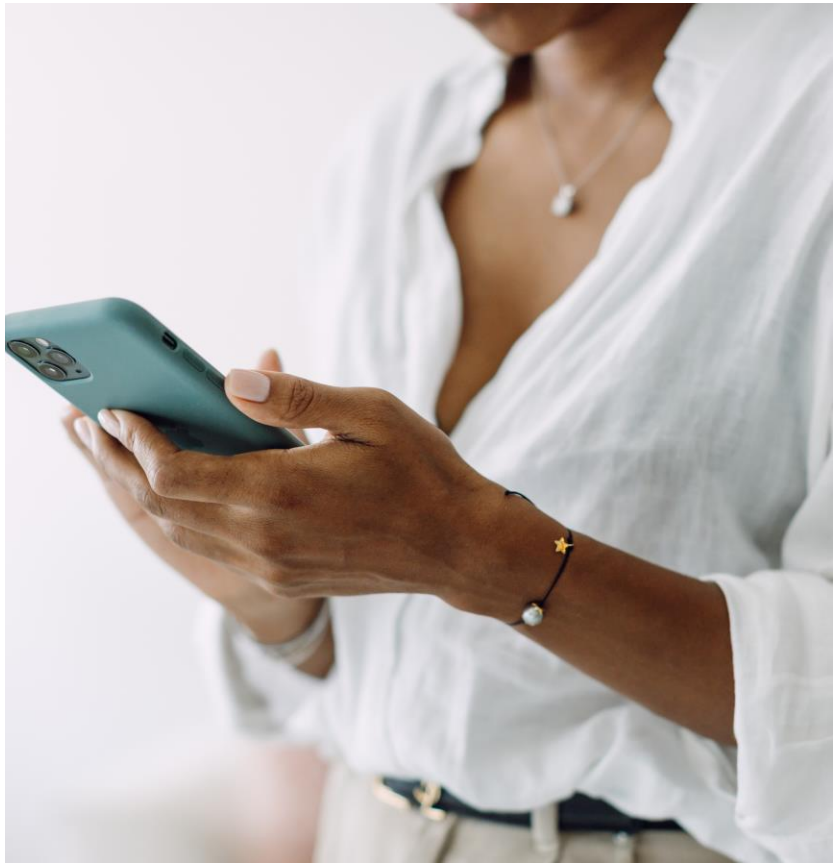
Law Enforcement and Cybersecurity Adaptation

- Struggling to hire and retain talent
- Public vs Private funding challenges
- Public- Private- Partnerships
- Community Model

Cybersecurity Impact on Staff

What your staff does matters

- Unsecure employee behaviour is the number 1 cause of breaches.
- More than 80% of breaches are due to human error.
- AI Chatbots mimic human emotions making scams more convincing.
- AI-Generated phishing click rates are 75% higher than regular phishing
- Generative AI tools enables attackers to make smarter more personalized scaled attacks.
- Cybersecurity Failures can cost you your client / Job!



AI Generated People

Business Email Compromise (BEC) Occurs When:

An attacker gains credentials to an email account

or

Impersonates a trusted entity

to

Manipulate employees, partners, clients or venders into taking harmful actions.

- Fake Invoice
- CEO/Executive/Authority figure impersonation
- Account compromise
- Data Theft
- Changing of Bank Details

Sometimes the account isn't taken over…
Lookalike Variations

- contact.us@calpeteclub.com
- contaetus@calpeteclub.com
- contaetus@calpeteclub.com
- contactus@calpetecluub.com
- contactus@calpetclub.com
- contactuss@calpeteclub.com
- contac.tus@calpeteclub.com
- contactus@calpete-club.cc
- contactus@calpetecluhb.com

BEC Tool AUTHREQUEST.io

IMPLEMENT ZERO TRUST

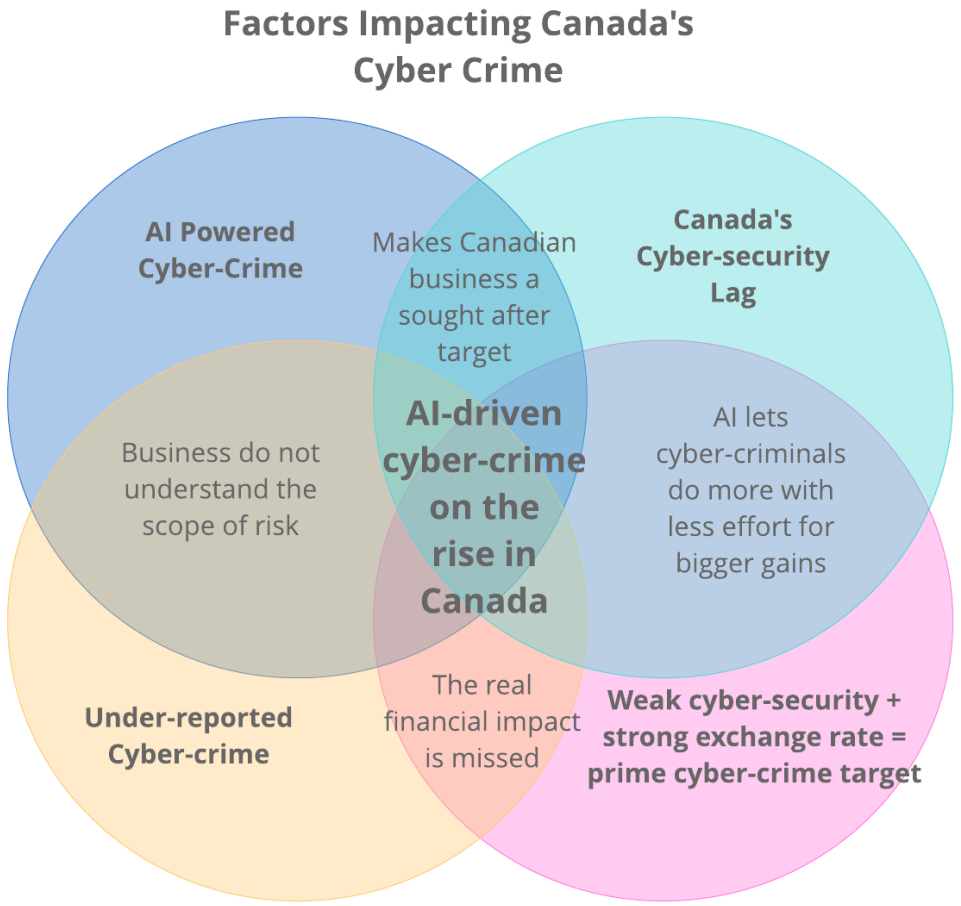
VERIFY REQUESTS: AUTHREQUEST.IO

HAVE A PLAN

Most understand to verify new interactions, however with the sophistication of AI, it's the trusted interactions and relationships that need as much or more verification

Are You or Your Client Prepared for AI Cyber Threats?

- Implement zero trust
- Use multi-factor authentication (MFA)-don’t pick your own passwords
- Get regular cyber assessment
- Get a BEC defense program
- Employee training that includes AI risks – Train by department



Key Drivers making Canada an increased target for AI Cyber-Crime

Thank you!

s01ve

Cyber Solutions

s01ve.io

1.844.828.3393

Path to RIMS Canada: the SARIMS Student Engagement Challenge

SARIMS
Southern Alberta Risk & Insurance Management Society

@SOUTHERNALBERTARIMS

RIMS CANADA CONFERENCE™
CALGARY 2025 | SEPTEMBER 14-17

Registration coming soon

Thank You to Our Sponsors

Platinum

AIG
AON
Gallagher Energy Risk Services
BHSI

Gold

Liberty Mutual INSURANCE
SOMPO
prl insurance brokers & advisors
Marsh
ZURICH

Silver

CHUBB
W A McLarens Company
IRIDIUM RISK SERVICES EVOLVED
NAVACORD