OSINT IN THE CONTEXT OF

INSIDER THREAT, INSIDER BREACH & INSIDER RISK MANAGEMENT

A Canadian Legal & Operational Perspective

A Practitioner's Reference Guide

Date: June 2026 | Version 1.0

Classification: RESTRICTED – For Security Practitioners Only

Presented by: Wolfhound Consulting and Investigation Services (WCIS)
https://wolfhoundcis.com

Table of Contents

1. Executive Summary

Open Source Intelligence (OSINT) has become an indispensable capability in the identification, investigation, and mitigation of insider threats within Canadian public and private sector organizations. As insider incidents grow in cost and complexity, OSINT provides security, human resources, and legal teams with a structured means of gathering and analysing publicly available information to assess risk, detect anomalous behaviour, and respond effectively to breaches.

This document provides a comprehensive examination of how OSINT is applied across the insider threat lifecycle: from pre-employment screening and continuous monitoring, to breach attribution and post-incident investigation. Critically, it contextualises these practices within Canada's unique and evolving legal landscape, including PIPEDA, Quebec's Law 25, the Foreign Interference and Security of Information Act (FISIA), Bill C-26, and the Ontario Employment Standards Act.

Key findings include:

- Malicious insider breaches, while representing approximately 8% of all Canadian data breaches, are the most financially devastating – averaging $7.98 million (CAD) per incident.
- Canada's patchwork privacy framework creates significant compliance complexity for employers wishing to conduct OSINT-based employee monitoring.
- OSINT, when properly governed, is a lawful and powerful tool for insider risk programmes, provided it adheres to proportionality, necessity, and transparency principles.
- Emerging legislation – particularly FISIA (2024), Bill C-26, and Quebec Law 25 – is reshaping the environment in which OSINT-enabled security programmes must operate.

Key Statistic

According to KPMG Canada's 2024 Cyber Incidents & Intelligence Report, malicious insider breaches cost Canadian organizations an average of $7.98 million per incident – the highest per-incident cost of any breach type.

According to the joint Deloitte Canada and Canadian Insider Risk Management Centre of Excellence 2025 Insider Risk Management in Canada report, 73% of participating organization experienced at least one internal threat incident in the past year.

2. Introduction to OSINT

2.1 Definition and Scope

Open Source Intelligence (OSINT) is the systematic collection, processing, and analysis of information derived from publicly available sources. Unlike signals intelligence (SIGINT) or human intelligence

(HUMINT), OSINT does not require covert methods or special legal authorisation to collect information – it relies solely on data that is openly accessible.

Sources of OSINT include:

- Social media platforms (LinkedIn, Facebook, X/Twitter, Instagram, TikTok)
- News media, blogs, and online publications
- Academic papers, patent databases, and research repositories
- Court records, property registries, and corporate filings
- Dark and deep web forums and marketplaces
- Job postings, salary databases, and professional associations
- Leaked credential databases and paste sites
- Domain registration (WHOIS) and DNS records
- Geospatial data and satellite imagery

OSINT is utilised by a diverse range of actors: national security agencies (CSIS, CSE), law enforcement (RCMP), corporate security teams, HR professionals, legal departments, and threat intelligence firms.

2.2 OSINT Categories and Techniques

OSINT methodology is broadly categorised into three operational approaches:

Approach	Description and Application
Passive OSINT	No direct interaction with the target or their systems. Involves reviewing public social media posts, news archives, court databases, and corporate registries. Carries the lowest legal and operational risk.
Semi-Passive OSINT	Involves minimal footprint interaction, such as accessing publicly indexed pages or non-targeted queries of open databases. Used in pre-employment due diligence and periodic risk assessments.
Active OSINT	Involves direct engagement with systems or individuals, such as API queries or targeted web scraping. Requires careful legal review, particularly under Canadian privacy law, as it may constitute collection of personal information.

Sub-disciplines of OSINT relevant to insider threat include:

- SOCMINT (Social Media Intelligence): monitoring of employee or candidate social media for indicators of discontent, externalisation, or ideological radicalisation.
- TECHINT (Technical Intelligence): scanning exposed IP ranges, credential dumps, and misconfigured cloud repositories for evidence of insider data exfiltration.
- FININT (Financial Intelligence - open source): reviewing public financial disclosures, bankruptcy filings, or litigation records that may signal financial distress and insider motivation.

- GEOINT (Geospatial Intelligence): analysing public location data to identify unusual travel or access patterns.

3. Understanding Insider Threats in the Canadian Context

3.1 Types of Insider Threats

The Canadian Security Intelligence Service (CSIS) and the Cybersecurity and Infrastructure Security Agency (CISA) broadly define an insider threat as the risk that a person with authorised access to an organisation's assets will use that access – intentionally or unintentionally – to cause harm. The principal categories are:

Insider Type	Characteristics
Malicious Insider	A current or former employee, contractor, or business partner who intentionally misuses access to steal data, commit sabotage, or facilitate external attacks. Often motivated by financial gain, ideology, coercion, or grievance.
Negligent Insider	An employee who inadvertently creates risk through careless behaviour: misconfiguring systems, falling for phishing attacks, losing devices, or mishandling sensitive data. The most common type by volume.
Compromised Insider	An individual whose credentials or systems have been taken over by an external threat actor, turning an unknowing employee into an attack vector.
Third-Party Insider	Vendors, contractors, and supply chain partners with privileged system access who may introduce risk through their own security posture or be deliberately exploited.
State-Directed Insider	Individuals acting at the direction of a foreign state or intelligence service to conduct economic espionage, sabotage, or to gather classified information. A specific concern for Canadian government and critical infrastructure.

3.2 The Insider Threat Landscape in Canada

Canada's geopolitical position as a G7 member and member of the Five Eyes intelligence alliance makes it a high-value target for foreign-state-sponsored insider activity. According to CSIS's 2024 Public Report, threats from foreign interference, espionage, and cyber activity continued to escalate in complexity throughout 2024, with hostile actors increasingly leveraging organised crime networks and state-sponsored actors.

From a commercial perspective, the landscape is equally concerning:

- Malicious insider breaches represent approximately 8% of all Canadian data breaches but carry the highest per-incident cost – averaging $7.98 million, according to the KPMG Canada 2024 Cyber Incidents & Intelligence Report.
- Breaches attributed to insiders between 2018 and 2020 increased by 47%, a trend attributed in part to the expansion of cloud computing environments that make insider detection more difficult.
- The Desjardins Group breach (2019) – Canada's most significant insider-caused financial data breach – went undetected for over 26 months, ultimately exposing the personal and financial data of 9.7 million individuals and resulting in a class-action settlement of approximately $201 million.
- The global average cost of insider threat incidents rose from $15.4 million (USD) in 2022 to $17.4 million in 2024, according to the Ponemon Institute's 2025 Cost of Insider Risks Global Report.

Former CSIS Official on Insider Threats

Former CSIS executive manager Dan Stanton described insider threats as "unquestionably the most serious threat to national security" in a February 2024 interview. He noted that insiders "progress from low-risk to potential to do some leakage to becoming a high-risk where they actually act on these impulses and these plans."

3.3 High-Profile Canadian Insider Cases

Several high-profile cases illustrate the severity and variety of insider threats in Canada:

- Desjardins Group (2019): A rogue employee exfiltrated the personal data of 9.7 million customers over more than 26 months before the breach was detected, following notification from the federal Privacy Commissioner. The case highlighted the risks of insufficient data access controls and prolonged undetected insider activity.

- Cameron Ortis / RCMP Intelligence (2019-2023): The former Director General of the RCMP's National Intelligence Coordination Centre was charged with unauthorised disclosure of classified information and offences under the Security of Information Act. Ortis was later convicted on multiple counts, representing a landmark prosecution of a high-trust insider within Canadian national security.

- Yuesheng Wang / Hydro-Québec (2022): Wang became the first person in Canada charged with economic espionage under the Security of Information Act, accused of stealing proprietary research from Hydro-Québec and communicating it to entities connected to China. This case underscored the risk of state-directed insiders in critical infrastructure and research organisations.

- Winnipeg National Microbiology Laboratory (2021): Two Chinese-Canadian scientists, Dr. Xiangguo Qiu and Dr. Keding Cheng, were removed from Canada's top biosecurity laboratory following an RCMP investigation into the alleged transfer of dangerous pathogens and potential espionage. This raised serious questions about insider screening in high-security research environments.

4. How OSINT Supports Insider Threat Detection

4.1 Pre-Employment and Onboarding Screening

OSINT plays a critical role in pre-employment due diligence, supplementing traditional background checks by providing a broader and more dynamic view of a candidate's digital footprint. This is particularly relevant for sensitive positions, roles involving access to classified information, and positions within regulated industries such as banking, telecommunications, and critical infrastructure.

OSINT-enhanced screening can reveal:

- Inconsistencies between stated employment history and verifiable online records (LinkedIn, corporate websites, professional association databases).
- Prior litigation, regulatory sanctions, or criminal proceedings accessible through public court databases (CanLII, provincial court registries).
- Public social media content indicating extremist ideology, financial distress, disgruntlement, or undisclosed foreign affiliations.
- Associations with known threat actors, sanctioned entities, or persons of concern identifiable through open-source databases (e.g., OFAC, Global Affairs Canada Controlled Persons List).
- Leaked credential exposure that may indicate prior security compromises or patterns of poor security hygiene (via tools such as Have I Been Pwned, dark web credential monitoring).

In Canadian government contexts, CSIS's Government Security Screening programme provides formal security assessments for individuals seeking security clearances at the Reliability, Secret, or Top Secret levels. OSINT is integrated into these assessments alongside HUMINT and records checks.

Legal Caution: Pre-Employment OSINT in Canada

Employers conducting OSINT-based screening must be cautious about collecting information that touches on protected grounds under provincial human rights codes (race, religion, family status, disability, etc.). In Alberta, under PIPA, and federally under PIPEDA, collection must be limited to what is necessary for the legitimate employment purpose. In Quebec, Law 25

requires explicit purpose specification. Employers should engage legal counsel and implement a documented screening protocol.

4.2 Continuous Monitoring and Behavioural Intelligence

OSINT is increasingly integrated into continuous employee monitoring programmes, enabling organisations to identify behavioural indicators of insider risk before a breach occurs. This approach recognises that insider threats are rarely impulsive – they typically follow a progression from predisposition to precursor behaviours to active harm.

Behavioural indicators identifiable through OSINT monitoring may include:

- Public posts expressing anger, resentment, or hostility toward the organisation, management, or colleagues.
- Sudden public displays of unexplained wealth (luxury purchases, travel, real estate activity visible in social media or public registries).
- Evidence of contact with foreign government officials, intelligence-linked organisations, or sanctioned entities through public social media or professional networking sites.
- Job-seeking activity on public platforms (LinkedIn signals, posting resumes on public boards) that may indicate imminent departure and elevated exfiltration risk.
- Posts or forum activity on dark web or extremist platforms accessible via OSINT tools.
- Changes in public sentiment – including sudden ideological shifts – visible through social media analysis tools.

Effective continuous monitoring requires integration of OSINT signals with internal security data (DLP alerts, access logs, SIEM events) to produce a holistic insider risk score. This is typically managed by User and Entity Behaviour Analytics (UEBA) platforms augmented with open-source feeds.

4.3 Dark Web and Open Forum Monitoring

The dark web – accessible via anonymising networks such as Tor – functions as a marketplace for stolen credentials, sensitive organisational data, and insider-for-hire services. OSINT tools provide visibility into these environments without requiring direct infiltration, enabling security teams to detect early warning signs of insider-enabled breaches.

Dark web OSINT can identify:

- Organisation-specific credentials, intellectual property, or internal documents offered for sale on dark web forums or marketplaces.
- Employees or contractors actively offering inside access or data to external buyers.
- Leaked internal data already in circulation, enabling rapid breach attribution.
- Threat actor discussions referencing specific Canadian organisations as targets.

Tools such as Recorded Future, DarkOwl, and Mandiant Threat Intelligence provide automated dark web monitoring capabilities. Open-source alternatives include manual monitoring of forums such as BreachForums and onion-site paste repositories.

4.4 Digital Footprint and Social Media Analysis (SOCMINT)

Social Media Intelligence (SOCMINT) is a sub-discipline of OSINT focused on deriving intelligence from social media platforms. In the insider threat context, SOCMINT enables organisations to monitor publicly available employee communications for indicators of risk.

Key SOCMINT applications include:

- Sentiment analysis of public posts to detect escalating grievances or disengagement trajectories.
- Network analysis to identify potentially problematic associations with foreign entities, competitors, or criminal networks.
- Geolocation analysis of tagged images or check-ins that may reveal unauthorised access to restricted locations.
- Identification of individuals selling sensitive information or credentials on public forums or social marketplaces.

Platforms such as Maltego, Skopenow, and Palantir provide automated SOCMINT aggregation and visualisation capabilities that are widely used by Canadian law enforcement and corporate security teams.

4.5 Technical Footprinting and Credential Exposure

OSINT enables technical security teams to identify exposed assets and compromised credentials that may indicate or facilitate insider activity:

- Shodan and Censys scanning can identify publicly exposed internal systems, cloud storage buckets, or misconfigured applications that insiders could exploit or have already exfiltrated data through.
- Certificate Transparency Logs (e.g., crt.sh) can reveal shadow IT infrastructure established by insiders.
- GitHub and other public code repositories can expose sensitive internal credentials, API keys, or proprietary code inadvertently or deliberately posted by insiders.
- Credential monitoring services (e.g., SpyCloud, Have I Been Pwned) can detect when employee credentials appear in public data breaches, indicating compromise risk.

5. OSINT in Insider Breach Response

5.1 Incident Detection and Attribution

When a potential insider breach is detected – whether through internal monitoring, external notification, or OSINT signals – OSINT plays a critical role in rapid attribution and scope assessment. Unlike externally-sourced breaches, insider incidents benefit from the availability of richer open-source data about the individual involved.

OSINT-driven attribution activities during a breach investigation may include:

- Correlating internal access logs with public evidence of the insider's activities (e.g., job applications to competitors, public posts indicating financial motivation, foreign travel).
- Identifying whether stolen data has been advertised or sold on dark web markets.
- Mapping the insider's external network through social media and professional platforms to identify potential co-conspirators or intended recipients of stolen information.
- Reviewing public court records, regulatory filings, or media reporting for any prior history of similar behaviour.

The evidential value of OSINT in Canadian criminal and civil proceedings requires careful chain-of-custody documentation. Investigators must record the exact source, collection method, timestamp, and content of each OSINT artefact to ensure admissibility and legal integrity.

5.2 Post-Breach Intelligence Gathering

Following a confirmed insider breach, OSINT continues to provide value in understanding the full scope of the incident and supporting remediation:

- Monitoring for continued distribution or sale of exfiltrated data on open and dark web channels.
- Identifying downstream victims of data that may have been shared, enabling notification obligations under PIPEDA's mandatory breach reporting requirements (MBRS) to be properly scoped.
- Gathering intelligence about the external actor or entity that may have directed or received the insider's activities, particularly in suspected state-directed espionage cases.
- Informing regulatory reporting to the Office of the Privacy Commissioner of Canada (OPC), provincial privacy commissioners, or – in critical infrastructure sectors – to the Canadian Centre for Cyber Security (CCCS).

6. OSINT and Insider Risk Management Programmes

6.1 Building an Insider Risk Programme in Canada

A mature Insider Risk Management (IRM) programme integrates OSINT capabilities across the full threat lifecycle: prevention, detection, response, and recovery. In the Canadian context, any such

programme must be structured to comply with the country's layered privacy law framework while delivering effective security outcomes.

Core components of a Canadian IRM programme include:

- Governance: An Insider Threat Policy endorsed at the executive level, defining the scope, purpose, and legal basis of monitoring activities. Requires input from legal, HR, IT security, and privacy functions.
- Defined Personas and Risk Indicators: Documented behavioural indicators informed by frameworks such as CERT's Insider Threat Common Sense Guide, adapted to reflect Canadian legal constraints.
- Technology Infrastructure: Integration of UEBA platforms, DLP solutions, SIEM, and OSINT tooling with clear data retention and access controls.
- OSINT Capability: A defined and legally governed process for conducting open-source research on employees and candidates, limited to specific triggering criteria and conducted by trained personnel.
- Cross-Functional Response Team: Integration of HR, Legal, IT Security, and physical security functions for coordinated response to insider incidents.
- Employee Awareness: Training programmes that communicate monitoring policies transparently and foster a security-conscious organisational culture.

6.2 Integrating OSINT into Risk Workflows

OSINT should be integrated into IRM workflows at defined trigger points rather than applied indiscriminately. A proportionate, triggered approach reduces privacy risk, legal exposure, and operational burden:

Workflow Stage	OSINT Integration Points
Pre-Hire Screening	Public social media review, credential exposure check, court records review, professional credential verification, sanctions list screening.
Onboarding / Clearance	Enhanced OSINT for sensitive roles; deep-dive digital footprint analysis for positions requiring security clearance.
Periodic Review	Annual or triggered re-screening for employees in high-risk roles (privileged access, classified information, executive positions).
Behavioural Trigger Response	Targeted OSINT investigation initiated upon specific behavioural indicators (e.g., sudden wealth, resignation, disciplinary action, access anomalies).
Active Investigation	Comprehensive OSINT investigation with documented chain of custody; coordinated with legal and HR.
Post-Incident Analysis	Dark web monitoring, data leak tracking, external entity mapping, support for PIPEDA breach notification assessment.

6.3 OSINT Tools Commonly Used

The following tools are widely deployed by Canadian security practitioners for insider threat-related OSINT:

Tool / Platform	Primary Application in Insider Threat Context
Maltego	Link analysis and network visualisation; mapping insider associations with external entities, threat actors, and foreign contacts.
SpiderFoot	Automated OSINT aggregation across 100+ sources; digital footprint analysis, credential exposure detection.
Shodan / Censys	Technical footprinting; identifying exposed internal assets, shadow IT, and misconfigured systems.
DarkOwl / Recorded Future	Dark web monitoring; detecting stolen credentials, data for sale, and insider-for-hire activity.
Skopenow	Social media and public records investigation; surface/deep/dark web coverage; employee due diligence workflows.
Have I Been Pwned / SpyCloud	Credential breach monitoring; identifying compromised employee accounts.
CanLII	Canadian legal database; reviewing prior litigation, regulatory sanctions, criminal history for persons of concern.
SEDAR+ / Canada Business Registry	Corporate registry intelligence; ownership structures, directorship histories, regulatory filings.
Palantir Gotham	Enterprise-grade link analysis and intelligence management; used by major Canadian financial institutions and government agencies.

7. Canadian Legal and Regulatory Framework

Canada's legal framework governing OSINT-based insider threat activities is complex, multi-jurisdictional, and rapidly evolving. Practitioners must navigate federal and provincial privacy statutes, human rights legislation, employment law, national security legislation, and criminal law simultaneously.

7.1 PIPEDA and Provincial Privacy Laws

The Personal Information Protection and Electronic Documents Act (PIPEDA) is the primary federal privacy statute governing private sector organisations in Canada. It establishes 10 Fair Information Principles (Schedule 1) that govern the collection, use, and disclosure of personal information.

PIPEDA applies directly to employee personal information only for federally regulated private-sector employers (banks, airlines, telecommunications companies, interprovincial transport). For provincially

regulated private-sector employers, PIPEDA does not apply to employee information in Alberta, British Columbia, and Québec, which have enacted "substantially similar" provincial legislation.

Key PIPEDA principles relevant to OSINT-based employee monitoring:

- Accountability (Principle 1): Organisations are responsible for all personal information under their control, including information collected through OSINT.
- Identifying Purposes (Principle 2): The purpose of collecting any personal information must be identified before or at the time of collection.
- Consent (Principle 3): Meaningful consent is generally required, though PIPEDA contains limited exceptions for investigations, fraud prevention, and national security.
- Limiting Collection (Principle 4): Collection must be limited to what is necessary for the identified purpose – a direct constraint on the scope of OSINT activities.
- Limiting Use, Disclosure, and Retention (Principle 5): Information collected for one purpose (e.g., recruitment) cannot be repurposed without consent (e.g., ongoing monitoring).
- Safeguards (Principle 7): Appropriate security safeguards must protect OSINT-derived data.

Key Compliance Gap

As noted by the Office of the Privacy Commissioner of Canada, significant gaps exist in statutory privacy protections for non-federally regulated employees in provinces without substantially similar legislation (notably Ontario and Nova Scotia). In these provinces, employee privacy protections are fragmented across employment standards legislation, privacy torts, employment contracts, and collective agreements – creating uncertainty for both employers and employees.

7.2 Quebec Law 25 (Loi Modernisant)

Quebec's Law 25 (Loi modernisant des dispositions législatives en matière de protection des renseignements personnels), substantially in force since September 2023, represents the most rigorous provincial privacy framework in Canada and is closely aligned with the EU General Data Protection Regulation (GDPR).

Law 25 provisions directly relevant to OSINT-based insider threat programmes include:

- Mandatory Privacy Impact Assessments (PIAs) before initiating any technology project that involves personal information – including OSINT-based monitoring tools.
- Explicit notice requirements when automated decision-making systems affect individuals' rights – directly relevant to AI-driven OSINT threat scoring platforms.
- Strengthened breach notification obligations to the Commission d'accès à l'information (CAI) and to affected individuals.

- Penalties of up to $10 million CAD or 2% of global annual turnover for contraventions, enforceable by the CAI.
- Data minimisation and purpose limitation principles that constrain the scope of open-source collection.

Federal Bill C-27, which would have replaced PIPEDA with the Consumer Privacy Protection Act (CPPA) and introduced the Artificial Intelligence and Data Act (AIDA), died on the order paper in January 2025 following Parliamentary prorogation. However, the underlying policy direction toward stronger privacy rights and AI regulation is expected to be revisited in future legislation.

7.3 Bill C-26 and the Critical Cyber Systems Protection Act

Bill C-26, An Act respecting cyber security, progressed through the Senate in late 2024 and introduced Canada's first legislative framework specifically targeting cybersecurity in critical infrastructure. It encompasses two principal components:

Amendments to the Telecommunications Act: Empowering the federal government to ban telecommunications service providers from using suppliers deemed "high-risk" – directly addressing supply chain and third-party insider risk.

The Critical Cyber Systems Protection Act (CCSPA): Imposing cybersecurity obligations on private sector entities in four federally regulated sectors: telecommunications, finance, energy, and transportation. Designated operators must:

- Establish and implement a cybersecurity programme.
- Identify and manage cyber security risks, including those arising from supply chains and third-party relationships.
- Report cybersecurity incidents to the relevant regulatory authority.
- Cooperate with government inspections and audits.

For OSINT and insider risk practitioners, the CCSPA creates a compliance obligation to proactively identify insider risk within supply chains and to have documented programmes in place – elevating OSINT-driven third-party screening from best practice to regulatory requirement in covered sectors.

7.4 Foreign Interference and Security of Information Act (FISIA)

Formerly the Security of Information Act (SOIA), the Foreign Interference and Security of Information Act (FISIA) was substantially amended by Bill C-70, the Countering Foreign Interference Act, which received Royal Assent on June 20, 2024 with amendments coming into force on August 19, 2024.

FISIA is the primary criminal law instrument addressing state-directed insider threats. It criminalises:

- Espionage: the communication of classified government or special operational information to a foreign entity.

- Economic espionage: the communication of trade secrets and intellectual property to foreign entities for the benefit of a foreign state.
- Foreign-influenced threats or violence.
- Preparatory acts in advance of espionage offences.

The 2024 amendments significantly modernised FISIA, including:

- Expanded offences addressing foreign interference in democratic processes.
- Enhanced penalties, including life imprisonment for the most serious espionage offences.
- Broader definition of "special operational information" to address military technology and knowledge.

For OSINT practitioners investigating suspected state-directed insider threats, FISIA establishes the criminal legal framework that may govern prosecution outcomes. Investigations involving suspected FISIA offences should be referred to RCMP and CSIS at the earliest opportunity.

7.5 Canadian Security Intelligence Service Act

The CSIS Act (R.S.C. 1985, c. C-23), as amended by the 2024 Countering Foreign Interference Act, governs Canada's national security intelligence community. Key provisions relevant to insider threat include:

- CSIS's mandate to investigate threats to the security of Canada, including espionage, sabotage, and foreign-influenced activities.
- The Government Security Screening programme, which authorises CSIS to conduct background investigations and provide security assessments for federal government employees and contractors requiring security clearances.
- Amended powers to share threat intelligence with provincial governments, municipalities, corporations, and individuals when they are the subject of specific threats – a significant expansion enabling OSINT-driven threat intelligence to flow more effectively to non-government organisations.
- CSIS's ability to share threat intelligence with Canadian academic and research institutions, addressing documented espionage risks at universities and national laboratories.

7.6 Ontario Employment Standards Act – Electronic Monitoring

Ontario is the only Canadian province with a statutory requirement for employers to maintain a written Electronic Monitoring Policy under the Employment Standards Act, 2000 (ESA). Since October 2022, Ontario employers with 25 or more employees must:

- Have a written electronic monitoring policy describing whether and how employees are monitored.
- Describe the types of electronic monitoring conducted.

- State the purposes for which the information gathered through electronic monitoring may be used.

While the Ontario ESA does not restrict the types of monitoring that may be conducted, the transparency and documentation requirements create a framework that effectively constrains ad hoc OSINT-based monitoring of employee online activities. Practitioners must ensure that any ongoing OSINT monitoring of Ontario employees is documented, purposeful, and disclosed in the Electronic Monitoring Policy.

7.7 Canadian Human Rights and Labour Considerations

OSINT-based screening must comply with applicable human rights legislation at both federal and provincial levels, including the Canadian Human Rights Act (federal) and provincial human rights codes. Key considerations include:

- OSINT screening must not collect or rely upon information related to protected characteristics (race, religion, gender, sexual orientation, disability, family status, etc.) in employment decisions.
- Social media screening, which frequently surfaces protected characteristic information, presents significant human rights risk and should be conducted by a designated third party operating under a structured protocol to limit exposure of the hiring decision-maker to protected information.
- Unionised workplaces may have collective agreement provisions that restrict or govern monitoring activities. Labour arbitrators in Canada have consistently applied a test of reasonableness, proportionality, and necessity to employer monitoring programmes.
- The OPC has noted that intense monitoring disproportionately affects lower-income workers, younger workers, persons with disabilities, and racialized workers – raising equity concerns that Canadian IRM practitioners must address in programme design.

8. Ethical Considerations for Canadian Practitioners

OSINT-based insider threat programmes raise significant ethical questions that extend beyond strict legal compliance. Canadian practitioners are encouraged to adopt a principled framework that balances organisational security needs against employee dignity, trust, and fundamental rights.

Key ethical principles for Canadian IRM practitioners:

- Proportionality: OSINT monitoring activities should be proportionate to the demonstrated risk. Blanket monitoring of all employees, or monitoring that exceeds what is necessary to address a defined risk, is ethically and legally problematic.

- Necessity: Each OSINT activity should be necessary to achieve a legitimate security purpose. Collecting information beyond what is required – even if publicly available – violates the spirit of Canadian privacy law and erodes organisational trust.

- Transparency: Employees should be aware that publicly available information may be reviewed as part of their employment relationship. This does not require disclosure of specific monitoring activities, but it does require honest policy communication.

- Fairness and Accuracy: OSINT data can be inaccurate, outdated, or misattributed. Security and HR professionals must implement verification protocols before taking adverse action based on open-source findings.

- Non-Discrimination: OSINT activities must not be designed or applied in a manner that produces discriminatory outcomes based on protected characteristics.

- Minimisation of Chilling Effects: Overly broad monitoring of employee social media or online activities can suppress legitimate speech and free expression, damaging organisational culture and potentially giving rise to legal claims.

OPC Guidance on Employee Monitoring Ethics

The Office of the Privacy Commissioner of Canada has noted that organisations have a legitimate interest in ensuring the security of their systems and information, but has consistently emphasised that monitoring should be narrowly tailored, proportionate to the risk, and clearly communicated to employees. The OPC has also cautioned against the use of invasive monitoring technologies that exceed what is necessary to achieve legitimate security objectives.

9. Best Practices and Recommendations

Based on the foregoing analysis, the following best practices are recommended for Canadian organisations implementing OSINT-enabled insider risk management programmes:

Governance and Policy

- Develop a formal Insider Threat Programme Policy that defines scope, legal basis, governance structure, and accountability mechanisms.
- Establish a multi-disciplinary Insider Threat Working Group comprising Security, HR, Legal, Privacy, and IT leadership.
- Document all OSINT activities, including purpose, methodology, tools used, data sources, findings, and disposition – this is essential for legal defensibility.

- Conduct annual legal reviews of the IRM programme against the evolving Canadian privacy and cybersecurity landscape.

Legal and Privacy Compliance

- Conduct a Privacy Impact Assessment (PIA) before implementing any OSINT tool or monitoring programme; this is mandatory under Quebec Law 25 and best practice nationwide.
- Establish a proportionality standard for OSINT activities: document why each type of monitoring is necessary for the specific security purpose.
- Engage qualified legal counsel with expertise in Canadian privacy, employment, and national security law when designing and reviewing IRM programmes.
- Maintain and regularly update an Ontario-compliant Electronic Monitoring Policy (mandatory for Ontario employers with 25+ employees).
- Do not rely solely on OSINT findings to make adverse employment decisions; corroborate with internal data and conduct a fair investigation process.

Operational OSINT Practices

- Implement a triggered approach to OSINT monitoring: define specific behavioural, technical, or contextual indicators that authorise enhanced open-source investigation.
- Train all personnel conducting OSINT investigations on Canadian legal constraints, ethical principles, and proper documentation practices.
- Separate OSINT screening from hiring decision-makers when conducting social media background checks to reduce human rights liability.
- Integrate OSINT feeds with internal UEBA, DLP, and SIEM platforms to contextualise open-source signals alongside internal behavioural data.
- Maintain dark web monitoring capability to detect early warning signs of insider-enabled data exfiltration.

Incident Response Integration

- Incorporate OSINT into breach response playbooks with clear roles, responsibilities, and legal review triggers.
- Establish escalation protocols for suspected FISIA or Criminal Code offences: preserve evidence, restrict system access, and engage RCMP and CSIS as appropriate.
- Ensure PIPEDA mandatory breach reporting assessments consider OSINT-derived intelligence about the scope and impact of insider-caused breaches.

Culture and Awareness

- Invest in security awareness training that addresses insider threat behaviours, reporting mechanisms, and the psychological dimensions of insider risk.
- Foster a reporting culture that enables employees to raise concerns about colleague behaviour without fear of retaliation.
- Address the root causes of insider risk (job dissatisfaction, financial stress, disengagement) through proactive HR, Employee Assistance Programme (EAP), and management practices.

10. Conclusion

OSINT represents one of the most powerful and cost-effective tools available to Canadian organisations seeking to manage the persistent and growing risk of insider threats. Its application spans the full spectrum of insider risk management: from pre-employment screening and continuous behavioural monitoring, to breach detection, attribution, and post-incident intelligence gathering.

However, in the Canadian context, OSINT cannot be deployed in isolation from a sophisticated understanding of the country's layered and evolving legal framework. The interaction between PIPEDA, provincial privacy laws (particularly Quebec's Law 25), the FISIA, the CSIS Act, Bill C-26's emerging cybersecurity obligations, and provincial employment law creates a compliance landscape that is uniquely challenging and demands proactive, expert legal engagement.

The consequences of getting this balance wrong are significant: organisations that over-monitor employees without proper legal authority expose themselves to regulatory sanction, civil liability, and reputational harm. Conversely, organisations that under-invest in OSINT-driven insider risk capabilities leave themselves vulnerable to the most financially and operationally devastating category of cyber incident in the Canadian landscape.

The most effective Canadian insider risk programmes will be those that treat OSINT not as a surveillance mechanism, but as an intelligence discipline: structured, purposeful, legally governed, ethically grounded, and integrated into a broader programme of prevention, detection, and response. As Canada's adversaries – whether foreign state actors, organised crime, or disgruntled employees – continue to exploit the insider vector, the organisations that respond with intelligence-led, rights-respecting programmes will be best positioned to protect their people, their data, and their competitive and national security interests.

11. References and Further Reading

Canadian Legislation and Regulation

- Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5.
- Quebec Act respecting the protection of personal information in the private sector (Law 25 / Loi Modernisant), as amended 2021.
- Foreign Interference and Security of Information Act (FISIA), R.S.C. 1985, c. O-5, as amended by Bill C-70 (2024).
- Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23, as amended.
- Bill C-26, An Act respecting cyber security (Critical Cyber Systems Protection Act), 44th Parliament, 1st Session.
- Employment Standards Act, 2000, S.O. 2000, c. 41 (Ontario) – Electronic Monitoring provisions.
- Canadian Human Rights Act, R.S.C. 1985, c. H-6.

Government and Regulatory Sources

- CSIS Public Report 2024. Canadian Security Intelligence Service, June 2025.
- CSE Annual Report 2024-2025. Communications Security Establishment Canada.
- Protecting Employee Privacy in the Modern Workplace. Office of the Privacy Commissioner of Canada, 2023.
- PIPEDA Requirements in Brief. Office of the Privacy Commissioner of Canada.
- Issue Sheets on Bill C-26. Office of the Privacy Commissioner of Canada, February 2024.
- Employee Monitoring in the Private Sector. Office of the Information and Privacy Commissioner of BC.
- Laws to Counter Foreign Interference. Public Safety Canada, 2024.

Research and Industry Reports

- Deloitte Canada and Canadian Insider Risk Management Centre of Excellence joint industry report on Insider Risk Management in Canada, September 2025.
- KPMG Canada. Cyber Incidents and Intelligence 2023 – March 2024. KPMG LLP, 2024.
- Ponemon Institute. 2025 Cost of Insider Risks Global Report. Proofpoint, 2025.
- IBM Security. Cost of a Data Breach Report 2024.
- Dolden Wallace Folick LLP. Cyber Risk: Current Landscape of Personal Information and Privacy Liability in Canada, February 2024.

Legal and Professional Commentary

- Employee Monitoring in Canada: What Employers Need to Know. Lexology / Labour and Employment Law Blog, February 2026.
- Social Media Screening for Job Applicants: Human Rights and Privacy Risks. Miller Thomson LLP.
- Practical Steps to Help Your Business Prepare for Quebec's Law 25 and Federal Bill C-27. Miller Thomson LLP.

- Canadian Cybersecurity Law Update: Bill C-26 Gains Momentum. Blake, Cassels & Graydon LLP, 2024.
- Addressing Insider Threats: The Role of HR in Employee Monitoring. Talent Canada, May 2025.

OSINT and Threat Intelligence Resources

- CERT Division, Carnegie Mellon University. Common Sense Guide to Mitigating Insider Threats, 7th Edition.
- Canadian Insider Risk Management Centre of Excellence, Professional Certificate.
- Group-IB. OSINT: Open Source Intelligence, Frameworks, and Cybersecurity Applications, 2025.
- SentinelOne. What is OSINT (Open Source Intelligence)? 2025.
- Syteca. 7 Real-Life Data Breaches Caused by Insider Threats, 2023.
- Skopenow. OSINT Workflows for Insider Threats (Webinar Series), 2025.

12. Contact the Insider Risk Management Centre of Excellence

For more information on Insider Risk Management, consult the Canadian Insider Risk Management Centre of Excellence (CInRM COE), your regional centre, or the Insider Risk Practitioner Alliance (IRPA) at:

- Insider Risk Practitioner Alliance (IRPA) – https://www.irpa.org/
- Canadian Insider Risk Management Centre of Excellence (CInRM COE) – https://www.cinrmcoe-cdecgrin.ca/
- United States Insider Risk Management Center of Excellence (USInRM CoE) – https://www.usinrmcoe.org/
- Australian Insider Risk Centre of Excellence (AIR CoE) – https://www.cybercollaboration.org.au/collaboration-partnerships/australian-insider-risk-centre-of-excellence-air-coe/
- UK Insider Risk Management Collaboration Centre (UKInRM CC) – https://www.ukinrmcc.uk/
- Norwegian Insider Risk Management Centre of Excellence (NInRM CoE) – https://www.ninrmcoe-nie.no/
- Swedish Insider Risk Management Centre of Excellence (SInRM CoE) – https://www.sinrmcoe-ski.se/
- Coming soon: New Zealand