

February 02, 2021

ARTICLE

Privacy Commissioner Report – Guidance for managing insider threats

Employees and other insiders are a significant risk to the security of personal information and other data. A substantial portion of cybersecurity incidents is caused or facilitated by the affected organization's insiders, whether acting inadvertently or intentionally. The Privacy Commissioner of Canada recently issued a report that provides guidance for managing insider threats.

Insider threats

Studies consistently indicate that a substantial portion of cybersecurity incidents and data breaches is caused or facilitated by a current or former insider (e.g., a director, executive/manager, employee or contract worker) of the affected organization or its business partners. For example, the *2020 Ponemon Cost of Insider Threats Global Report* concludes that the frequency and cost of insider threats have increased dramatically over the course of two years.

An organization's insiders present significant risk because they have authorized access to the organization's information technology systems, knowledge of the organization's valuable data and security practices, and a greater window of opportunity for misconduct. Those circumstances can enable an insider to engage in misconduct that is harder to detect and remedy, and results in more harm, than external threats.

Insiders can cause or facilitate a cybersecurity incident or data breach inadvertently (e.g., due to mistake or manipulation by other persons) or deliberately for various motives (e.g., financial gain, malice or enjoyment). Regardless of whether an insider's actions are inadvertent or deliberate, the results can be the same – potentially devastating harm to the organization, potentially significant liabilities by the organization to individuals and other organizations harmed by the incident, and potentially significant fines imposed on the organization by regulators.

Effective insider threat management requires a risk-based, multi-functional approach by an organization's various departments and disciplines to deter, prevent, detect and respond to cybersecurity incidents and data breaches caused by insiders. Government agencies and organizations have issued best practices guidance for managing insider threats, including *How To Protect Your Organization From Insider Threats* issued in February 2020 by the Canadian Centre for Cyber Security. For more information, see BLG bulletin *Managing Insider Risk – Recent Best Practices Guidance*.

Privacy Commissioner investigation report

In December 2020, the Office of the Privacy Commissioner of Canada (the OPC) issued an *investigation report* regarding a financial institution's compliance with PIPEDA relating to a breach of security safeguards that affected the sensitive personal information of close to 9.7 million individuals. The breach was caused by one of the financial institution's employees, who intentionally exfiltrated personal information for at least 26 months.

The financial institution had established systems and practices designed to protect personal information, including technological measures to restrict access to personal information stored in data warehouses. However, the measures did not prevent well-meaning authorized employees from transferring personal information from the warehouses to shared drives that were not fully protected. The malicious employee, a "skilled and high performing" employee who was a trusted resource for many of his colleagues, was not authorized to access the data warehouses but could access personal information that other employees had downloaded to shared drives. The malicious employee transferred personal information from shared drives onto personal removable storage devices (i.e., USB keys) and then disclosed the information to third parties.

In its report, the OPC reviewed the financial institutions' policies, practices and procedures to protect the security and confidentiality of personal information. The OPC commended the financial institution for its trusting relationship with its employees but cautioned that an organizational "climate of trust" must be accompanied by a "culture of vigilance" that "adopts verification and control measures". The OPC further explained that an organization must have a "culture of accountability".

The OPC cautioned that the "human factor is the weakest link when it comes to information protection in a technological environment". The OPC noted that breaches caused by insiders "are more difficult to prevent than attacks caused by external threats, in particular because they are the work of technically competent employees who know the company's systems and security weaknesses, where information is located, and how to circumvent the protective processes in place".

The OPC emphasized the need for vigilance and a holistic approach when deploying measures to address and mitigate the impact of insider threats. The OPC detailed several recommended measures to combat insider threats. Following is a summary.

- Security screening/confidentiality agreements: Security screening (before hiring employees, when transferring employees to a new position and periodically for certain employees) to identify job candidates or employees with suspicious backgrounds or conduct that make them unsuitable to be given access to certain resources, and confidentiality agreements specific to assigned duties and annual code of conduct attestations.
- Organizational policies and procedures: Personal information security policies and procedures applied appropriately and consistently and that enable verification of employee compliance.
- Employee training and awareness: Employee awareness of the importance of personal information confidentiality and the serious consequences of violating personal information confidentiality. Sufficient training (e.g., training for new employees and ongoing training and awareness programs for all employees) to enable employees to understand and effectively implement the organization's information security policies and procedures, and measures to demonstrate the effectiveness of the training.
- Access controls and data segregation: Organizational and technological measures to protect personal information, including measures to manage data access rights and data segregation.
- Oversight and monitoring: Oversight and monitoring (e.g., technological measures such as active information system monitoring, a user and entity behaviour analytics solution, logging and a data loss prevention solution) to detect suspicious uses of resources and employees' potential non-compliance with the organization's directives and policies and to detect and prevent the exfiltration of sensitive data.

The OPC concluded that the financial institution contravened PIPEDA requirements for safeguarding personal information. In particular, the OPC found: (1) the financial institution had many data security directives, policies, and procedures, but some were either incomplete or not properly implemented; (2) there were critical gaps in the financial institution's employee training and awareness; (3) the financial institution did not effectively

manage data access rights and data segregation; (4) the financial institution had not fully implemented systems to detect and prevent unauthorized access to and exfiltration of data; and (5) the financial institution had not implemented appropriate data retention periods or procedures for the destruction of personal information.

The OPC recommended that the financial institution remedy identified deficiencies and engage an accredited and experienced external auditing firm to assess and certify the institution's information security and privacy program. The financial institution accepted the OPC's recommendations.

Comment

Organizations should evaluate their insider threat management program in light of best practices guidance and make appropriate improvements with an emphasis on protecting the organization's high-value assets and areas of highest risk.

When establishing and implementing an insider threat management program, organizations should be mindful of legal compliance requirements, including compliance with privacy/personal information protection laws, labour/employment laws and human rights laws. Timely legal advice can help an organization address those legal compliance requirements. In addition, the involvement of lawyers in certain insider threat management activities (e.g. assisting in the preparation or review of relevant policies/procedures and conducting testing/training activities) is necessary to establish legal privilege over communications regarding those activities. For more information, see BLG bulletins [*Cyber Risk Management – Legal Privilege Strategy \(Part 1\)*](#); [*Cyber Risk Management – Legal Privilege Strategy \(Part 2\)*](#); [*Legal Privilege for Data Security Incident Investigation Reports*](#); and [*Loss of Legal Privilege over Cyberattack Investigation Report*](#).

Organizations should also consider whether they have appropriate insurance for losses and liabilities resulting from insider threats. For more information, see BLG bulletin [*Insurance for Cybersecurity Incidents and Privacy Breaches*](#).

Services: [Cybersecurity, Privacy & Data Protection](#), [Compliance with Privacy & Data Protection](#)

Key Contacts

Robert J.C. Deane
Partner

 Vancouver

 RDeane@blg.com

 [604.640.4250](tel:604.640.4250)

Related Content

[Managing Insider Risk - Recent Best Practices Guidance](#)

[Insurance for Cybersecurity Incidents and Privacy Breaches](#)