Opportunity Profile  Chief Information Security Officer

Liquor Distribution Branch

British Columbia
BC LIQUOR DISTRIBUTION BRANCH | CHIEF INFORMATION SECURITY OFFICER

CONTENTS

THE ORGANIZATION  BC LIQUOR DISTRIBUTION BRANCH  1
THE OPPORTUNITY  CHIEF INFORMATION SECURITY OFFICER  3
  Nature of Work and Position  4
  Specific Accountabilities / Deliverables  4
THE PERSON  6
  Education and Recent, Related Experience  6
  Knowledge  6
  Skills and Abilities  7
  Competencies and Personal Characteristics  7
COMPENSATION  8
CONTACT  8
THE ORGANIZATION

BRITISH COLUMBIA LIQUOR DISTRIBUTION BRANCH

The BC Liquor Distribution Branch (LDB) is one of two branches of government responsible for the cannabis and liquor industry in BC, operating the wholesale distribution of beverage alcohol and non-medical cannabis within the Province as well as the household retail brands of BC Liquor Stores and BC Cannabis Stores. As the sole buyer and re-seller of liquor in the Province of BC’s mixed public-private model under the Liquor Distribution Act, the LDB contributes more than $1 billion annually in revenue to the Province, providing financial support for a variety of vital public services such as health care, education, and social services.

With a workforce of approximately 5,000 full and part-time employees and operating 198 retail liquor stores and 25 retail cannabis stores across the province, the LDB is one of the largest retailers in BC, and sees more than 40 million retail customer visits annually. Every year, the LDB purchases beverage alcohol from over 1,000 Canadian and international suppliers and manufacturers, and supplies product to more than 10,000 BC bars, restaurants, wholesale customers, and private retailers.

The LDB is a unique government entity that operates with similar independence to a Crown Corporation under the direction of a General Manager and CEO. To best serve the interests of its customers and stakeholders, the LDB manages the importation, warehousing, and distribution of beverage alcohol to outlets throughout BC; promotes the safe and responsible use of beverage alcohol; and establishes sound policies to ensure the LDB develops and implements programs and services aimed at deterring the sale of beverage alcohol to minors.

To learn more, please visit the BC Liquor Distribution Branch’s website.
THE OPPORTUNITY

CHIEF INFORMATION SECURITY OFFICER

The information technology (IT) team is highly customer focused and directly supports four distinct lines of business: retail liquor, wholesale liquor, cannabis (wholesale & retail), and corporate services. These line of business technology teams are supported overall by both a Chief Information Security Officer and a Chief Technical Officer and their respective departments to ensure the organization prioritizes security and innovation, with common standards and technologies across all lines of business.

At present, the technology team consists of more than 200 full-time employees, and has also adopted a sourcing strategy to leverage external expertise where greater capacity is required for the Change Portfolio.

The teams integrate, maintain, and enhance more than 80 business systems on a hybrid on-premises and cloud infrastructure. These include:

- Merchandising and retail store systems that process 40 million plus customer transactions per year
- Wholesale, distribution, and warehouse systems that distribute 17 million+ cases annually
- Corporate finance systems to service an annual budget of approximately $3 billion and HR and payroll systems to service more than 5,000 employees.
THE OPPORTUNITY  CHIEF INFORMATION SECURITY OFFICER

Reporting to the Chief Information Officer, the Chief Information Security Officer (CISO) core responsibility is to oversee information risk management for the organization. The CISO is responsible for developing and implementing enterprise security and risk policies, monitoring vendor risks, and influencing user behavior. The CISO is also responsible for 24x7 security operations, network engineering, security tools engineering and disaster recovery planning. Other responsibilities include physical security, business continuity planning, crisis management, privacy, and compliance.

The CISO is the principal relationship manager for business executive and senior management staff for all aspects of IT Security and Business Continuity, in the context of the corporate risk management framework. This position is responsible for the achievement of corporate strategic plan objectives (as defined at CPIC), business continuous improvement (as defined at MPIC) and IT department objectives, as set on an annual basis. The CISO area is currently leading a multi year Cyber Security program with significant investment as part of the Corporate strategic plan.

The CISO is responsible for all aspects of technology, people, budget and process to ensure directorate objectives are met. The Director establishes the organization that will support the business including alternative methods of service delivery through third parties. The position is responsible for governance as it relates to legislation, regulation and developing LDB standards.
Accountabilities

Strategic

- Acts as a strategic advisor to business, IT Directors and the CIO. Provides expert advice and guidance in the identification of needs and fulfilment with technology based security solutions. Ensures that the projects delivered achieve a holistic solution approach by partnering with CTO and IT Director organizations. Acts with high autonomy and actively bring forward ideas and recommendations to further the success of the business lines.

- Oversees cross business line collaborations, development of IT Security strategy for all the technical activities of the organization. Establishes security and network architecture aligning business and technical capabilities into a clear and comprehensive vision with implementation strategies and delivery roadmaps. Leads the planning, development, and implementation of security frameworks and plans to improve incident prevention, detection, and response.

- Leads the department and ensure the alignment with and contribution to the Corporate Strategic Plan. Directs the identification of issues, sets goals and objectives, establishes work plans and tactics by leading the planning and implementation of corporate and departmental strategy and plans.

- Participates in the planning processes of the Branch. Develops policies and programs to respond to changes in business environments, legislation, public opinion and fiscal realities. Monitors the management of performance indicators that accurately reflect allocation of physical and human resources as they apply to delivery of services.

- Represents LDB on cross-government and cross-sector information security management and information security technology issues and policy development often requiring coordination of a variety of activities with officials of other ministries, central agencies, and broader public sector bodies. Works closely with the provincial CISO.

- Oversees the review of business programs and systems to identify non-compliance with policies and correct deficiencies; and the conduct of security checks for measurement and reporting. Provides leadership to multi year Cyber Security program, benchmarking externally against NIST standards.

- Provides oversight to ensure Recovery capabilities, leading disaster recovery planning and testing for all LDB business services.
Customer

- Advises business regarding the security of existing and proposed systems, considering new IT security and network approaches, and recommends enhancements and solutions. Develops and fosters effective working relationships with Government, suppliers and service providers to facilitate a smooth running service.

- Leads the development and implementation of information security technologies, policies, procedures, standards and training to minimize privacy and security risks to the ministry and its stakeholders. Working with the cyber security program manager, directs teams to lead project planning efforts including project definition, project justification, proposals, success criteria, risks/issues, requirements definition, technical design, testing procedures and documentation, system documentation, user training, and production delivery while coordinating and communicating with business and technical resources.

- Evaluates requests for security systems and network changes and enhancements, determines business feasibility, cost-effectiveness, resource requirements and impact on current and future systems, and recommends appropriate action.

- Conducts security, threat, and risk assessments for new systems and changes to existing systems.

- Investigates all security breaches to determine the source, method and damage that occurred. Reviews security event reports and determines if further investigation is required. Elevates to applicable authority and/or leads full review and reporting. Determines specific security needs of an investigation and requirements to grant or withhold access to data; ensures that data is properly preserved for presentation in court.

- Implements corrective measures to prevent recurrence of breaches; reviews and updates measures on an ongoing basis to ensure currency with new and emerging threats, and continuous improvement processes. Leads incident response and business continuity activities.

Financial

- Enables business operational revenues by demonstrating in-depth understanding of the complexities of the organization, processes, information and technologies and directs projects to best realize the organization strategy. Resolves complex challenges and ensures issue resolution and risk mitigation.
• Guides development and administration of annual operating budget including salary, administration expenses, ongoing hardware needs and software licenses. Identifies and implements methods of expense monitoring; provides leadership and direction to other departments to ensure optimum utilization of technical resources.

• Financial authority of an operating budget of circa. $6,000,000 and cyber security program budget of circa. $2,500,000 annually. Signing authority of $100,000 per occurrence (operating budget).

People

• Provides coaching and mentorship to the team, especially to develop their capabilities through a structured performance plan methodology.

• Oversees the ongoing leadership, training, development and succession planning of staff.

• Broadens out the breadth and depth of available SME pool via recruitment, rotation, cross skilling, training, and performance management of staff.

• Provides guidance, mentorship and technical expertise across multiple streams. Manages the group and its people through successful recruitment, performance management, development planning and retention of a high performing team.

• Improve employee engagement on an ongoing basis, focusing on identified development area for the Group. Run focus groups or alternative mechanisms to track progress and generate ideas.

• Directly supervises up to 5 - 7 management level full-time employees. Supervises up to 45 employees through subordinate supervisors.
THE PERSON

Education and Experience

- Degree in computer science or a related field.
- Professional designation as a Certified Information Systems Security Professional or Certified Information Security Manager, or equivalent experience.
- Minimum 10 years’ experience of recent, related experience:
  - Leading, coaching and managing diverse multi-disciplinary staff who may be located in geographically separated locations.
  - Experience in identifying and evaluating information management risks from a business and technological standpoint as a senior manager in a large organization.
  - Experience with strategic planning, implementation and organizational transformation.
  - Experience leading, mentoring and managing technical staff in a unionized work environment.
- An equivalent combination of education, training and experience may be considered, i.e., 15 or more years of the above listed experience combined with a diploma or certificate in computer science or a related field.

Knowledge

- Knowledge of threat and risk assessment processes; knowledge of current risks and threats; and knowledge of identity access management.
- Knowledge of security and network technologies (e.g., firewalls, routers, identity management, active directory, intrusion detection, privileged access management, event monitoring etc.)
- Knowledge of retail and wholesale business/operations are preferred.
- Knowledge of IT Service Management and Operations, preferably ITIL practices.
- Knowledge of IT Security Maturity accreditations, preferably NIST.
- Knowledge of IT Quality Assurance practices, preferably CMMI.
Skills and Abilities

- Demonstrated ability to set a vision collaboratively and inspire stakeholders to progressively adopt.
- Demonstrated ability to effectively lead people in effective collaborations to diagnose and resolve complex issues.
- Strong financial management skills in budgeting, forecasting, and cost control.
- Strong leadership skills and change management abilities.
- Excellent analytical, judgement, persuasion and consensus building abilities where there are competing interests.
- Demonstrated ability to develop and maintain productive relationships with individuals at various levels internally and externally.
- Ability to manage multiple priorities and produce results within deadlines.
- Knowledge of iterative and test-driven software development and continuous integration.
Competencies and Personal Characteristics

**Integrity** - Displays and promotes conduct and behaviours consistent with the BC LDB’s standards. Demonstrates a high level of emotional/intellectual acuity and leads by example, communicating clear goals and objectives; shows a resolute commitment to the rules and core values of the organization.

**Leadership** - Assumes responsibility for establishing clear team vision, goals and objectives; supports and motivates the delivery of high performance; enables direct reports in capacity and career development.

**Business Acumen** - Ability to understand the business implications of decisions and to strive to improve organizational performance. Requires an awareness of business issues, processes, and outcomes as they impact the client’s and organization’s business needs.

**Managing Organizational Resources** - Maintains an inventory of resources for the fulfilment of goals and objectives for various initiatives; obtains information and identifies key issues and implications to make informed, objective decisions.

**Impact and Influence** - Combines reasoned, realistic judgement and commitment to key outcomes; demonstrates a blending of visionary thought and drive with pragmatism and perseverance. Has an ability to maintain the commitment of others; relies upon self-confidence and insight to drive change and meet individual, situational, as well as organizational challenges.

**Partner with Stakeholders** - Anticipates, responds, and attends to the needs of both internal and external stakeholders of the organization, and treats all staff and stakeholders with respect; maintains enthusiasm and commitment in gaining support and cooperation from stakeholders, colleagues, external customers, and other parties.

**Change Leadership** - Involves creating a new vision for the organization and taking the required actions to ensure members of the organization accept and support the vision.

**Improving Operations** - Identifies and understands how internal and external issues (e.g. economic, political, social trends) impact the work of the LDB. Demonstrates knowledge/skill in fostering creative problem solving in the organization through critical reflection, problem analysis, risk assessment, and rewarding innovation.

**Holding People Accountable** - Holds self and others accountable for responsibilities; focuses on results and measuring attainment of outcomes in a business focus.
COMPENSATION

A competitive compensation package will be provided including a competitive base salary and excellent pension and benefits. Further details will be discussed in a personal interview.

FOR MORE INFORMATION PLEASE CONTACT:

Julian Manchon or Greg Longster
LEADERS INTERNATIONAL EXECUTIVE SEARCH
#880—609 Granville Street
Vancouver, BC  V7Y 1G5
Phone: (604) 688-8422
Email: vancouver@leadersinternational.com