Leaders INTERNATIONAL Executive Search

VANCOUVER EDMONTON CALGARY SASKATOON WINNIPEG TORONTO OTTAWA MONTREAL



Digital Commerce Group

Opportunity Profile

Vice President, Infrastructure & Chief Information Security Officer (CISO)

Location: Calgary, AB or Toronto, ON

About Digital Commerce Group

www.dcbank.ca

Digital Commerce Group (DCGroup) is a Calgary-headquartered financial technology group and a pioneer of Payments-as-a-Service in Canada. The group brings together Digital Commerce Bank (DCBank), a Schedule 1 Canadian chartered bank, Digital Commerce Payments Inc. (DCPayments) and Pateno Payments Inc. (Pateno). Its enterprise-grade payment and banking technology helps corporations, financial services providers and fintech entrepreneurs move money faster, more transparently and at lower cost than traditional financial services.

DCBank was incorporated in 2007 under the Bank Act and runs a 100% owned and operated technology platform with access to all major Canadian payment rails. The Bank is a member of Payments Canada and the Canada Deposit Insurance Corporation (CDIC), and a principal member of Interac, Visa and Mastercard. In 2025 it became the first bank in Canada to launch Interac e-Transfer Cards.

DCPayments and Pateno are affiliates of DCBank and use its access to the payment rails to deliver API-driven payment solutions, from merchant acquiring and 3D Secure card payments to Interac e-Transfer at online checkout, disbursements, rent and loan payments. Clients integrate these services directly into their own websites, portals and apps. Pateno serves niche markets with high-speed, high-volume payment needs.

DCGroup pairs the discipline of a regulated Canadian bank with an entrepreneurial culture built on experimentation and collaboration, growing through new products, partnerships and acquisitions.

Vice President, Infrastructure & Chief Information Security Officer (CISO)

Digital Commerce Group is seeking an experienced Vice President, Infrastructure & Chief Information Security Officer (CISO) to lead security across the group's banking and payments businesses. The position reports to the Chief Technology Officer (CTO) and can be based in either Calgary, Alberta or Toronto, Ontario.

This is first and foremost a CISO role. DCGroup sells secure money movement, and its products are APIs that clients plug directly into their own platforms, so security is part of the product rather than a back-office function. The VP & CISO owns the group's information security program end to end: cyber risk, API and application security, the secure adoption of AI, and the audit and compliance programs that underpin client, partner and regulator trust, including PCI DSS, SOC 2 Type II and regulatory examinations. The role also oversees infrastructure, cloud and technical client support for a 24x7x365 banking and payments operation.

The ideal candidate is a hands-on security executive who has led audits from the front, is fluent in API and cloud security, and brings a practical, risk-based approach to AI. They are as comfortable in front of auditors, regulators and executive leadership as they are with engineers and product teams, and they thrive in an entrepreneurial environment where the answer is rarely "no" but "here's how we do this safely."



Key Responsibilities

Security Strategy & CISO Leadership

- Serve as CISO for DCGroup, including DCBank, DCPayments and Pateno, and lead the enterprise information security and cybersecurity program.
- Own the information security strategy, governance model, policies, standards, control framework and multi-year security roadmap, aligned with the group's growth plans and risk appetite.
- Identify, assess and manage cyber and technology risk, and report clearly on risk posture, incidents, control effectiveness and security performance to the CTO, executive leadership and governance committees.
- Lead security operations, threat detection and monitoring, vulnerability management, penetration testing and incident response, including forensics coordination, containment, recovery and lessons learned.
- Act as the executive point of contact during significant cyber incidents, coordinating with leadership, legal, compliance, clients, regulators, payment networks, insurers and other stakeholders.
- Build a strong security culture through awareness programs, role-based training and phishing exercises, and partner with the business so security enables new products rather than slowing them down.

Audit, Compliance & Regulatory Assurance

- Own PCI DSS compliance across the group, including scoping, cardholder data environment controls, the annual assessment with the Qualified Security Assessor (QSA), the Report on Compliance and year-round evidence.
- Maintain and mature the control environment supporting SOC 2 Type II attestation and lead the organization through each examination period.
- Lead the technology and cyber components of regulatory examinations and internal and external audits, including alignment with OSFI's expectations for technology and cyber risk management (Guideline B-13).

- Drive timely remediation of audit findings, control deficiencies, security assessments and penetration-test results, with clear ownership and tracking through to closure.
- Meet the security requirements of payment networks and partners, including Interac, Visa and Mastercard.
- Oversee third-party and vendor risk, including security due diligence, contractual security requirements and ongoing monitoring of critical service providers.

API & Application Security

- Set the security standard for DCGroup's API platform, which clients use to embed payment and banking services directly into their websites, portals and apps.
- Oversee API security architecture and controls, including authentication and authorization (e.g., OAuth 2.0, mutual TLS), API gateway policy, rate limiting, input validation, secrets and key management, and protection against abuse and fraud.
- Embed security across the software development lifecycle (DevSecOps), including threat modelling, secure code review, static and dynamic testing, and dependency and supply-chain controls, in partnership with engineering and product teams.
- Lead regular API and application penetration testing, and security review of client and partner integrations before and after go-live.
- Protect sensitive financial and cardholder data through encryption, tokenization, data loss prevention and strong identity and privileged access management.

AI Security & Governance

- Develop and maintain AI acceptable-use policies, data handling standards and risk assessments for AI tools, models and vendors, aligned with emerging regulatory expectations for financial institutions.
- Assess and manage AI-specific risks, including data leakage, prompt injection, third-party AI risk, and AI-enabled fraud and social engineering.
- Apply AI and automation within the security function to strengthen threat detection, triage, monitoring and compliance evidence gathering.

Infrastructure & Operations

- Lead enterprise infrastructure services across Linux and Windows servers, storage, networking, cloud platforms, virtualization, databases, identity services, endpoint management and workplace technology.
- Ensure infrastructure meets the availability, resiliency, security, performance and scalability requirements of a 24x7x365 banking and payments operation.
- Own business continuity, disaster recovery and operational resilience, including defined and regularly tested recovery time and recovery point objectives.
- Maintain after-hours support, on-call coverage, escalation procedures and major incident management for critical services.
- Drive infrastructure modernization, automation, standardization and cost optimization, with security designed in from the start.



Technical Client Support

- Lead the Technical Client Support team, covering service desk, end-user technology, access support and technical assistance for internal and external stakeholders, with 24x7x365 coverage.
- Set and monitor service levels and KPIs, and mature IT service management practices across incident, problem, change, request, asset and knowledge management.
- Build a service culture focused on accountability, responsiveness and client experience.

The Person

Qualifications & Experience

- Significant progressive experience in information security, including senior leadership as a CISO or head of security, ideally within a bank, payments company, fintech or other regulated financial services organization.
- Hands-on experience leading PCI DSS assessments (working with QSAs through the Report on Compliance) and SOC 2 Type II examinations, with a track record of closing audit findings.
- Strong command of API and application security, secure SDLC and DevSecOps practices, and cloud security architecture.
- Practical experience setting policy and controls for the use of AI tools, and a working understanding of AI-related risks and emerging governance expectations.
- Experience working directly with regulators and auditors; knowledge of OSFI expectations for technology and cyber risk is a strong asset.
- Solid infrastructure grounding in mixed Linux and Microsoft Windows environments (roughly half of the server environment runs on Linux), VMware virtualization, cloud platforms, and identity and access management including Active Directory, Microsoft Entra ID and privileged access management.
- Experience supporting highly available, mission-critical systems in a 24x7x365 environment, including incident response, disaster recovery and operational resilience.
- Proven ability to build, lead and develop security, infrastructure and support teams.
- Professional certifications such as CISSP, CISM or CISA are considered an asset.

Core Competencies

- **Entrepreneurial mindset:** pragmatic, commercially aware and comfortable building and scaling programs in a growing organization.
- **Risk-based judgment:** knows when to hold the line and when to find a safe path to yes.
- **Hands-on leadership:** willing to roll up their sleeves, with a track record of building, coaching and holding teams accountable.
- **Clear communicator:** able to explain complex security and compliance issues to executives, auditors, regulators, clients and engineers.
- **Composure under pressure:** calm, decisive leadership during incidents and high-stakes situations.
- **Analytical rigour:** strong problem-solving, critical-thinking and troubleshooting skills.
- **Agility:** able to manage multiple priorities and shifting demands in a fast-paced environment.
- **Integrity:** high standards of confidentiality, ownership and professional conduct.

Compensation

A competitive compensation package will be provided. This role is based out of either the Toronto or Calgary offices. Remote consideration may be made for exceptional candidates who are not located in Calgary or Toronto. Relocation may be considered. Further details will be discussed in a personal interview.

Express Your Enthusiasm

Please email a convincing cover letter and tailored resume (PDF or Word document only) to **John Dugdale or Heather Fookes** at **apply@leadersinternational.com** indicating the job title in the subject line of the email.

Leaders International Executive Search
www.leadersinternational.com