INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-24 19:00 UTC

# London Hydro Data Breach Exposes Customer PII for 170,000 Customers

DATA BREACH | CRITICAL | CVSS 6.5

| | |
|---|---|
| SCC Item ID | SCC-DBR-2026-0200 |
| Type | Data Breach |
| Severity | CRITICAL |
| CVSS Base Score | 6.5 |
| Affected Products | London Hydro (Canadian electricity utility), customer account and personal information systems |
| Published | 2026-06-23 |
| Discovery Source | Gemini |

## Executive Summary

On June 20, 2026, London Hydro, a Canadian electricity utility serving approximately 170,000 customers, suffered a data breach that exposed customer names, postal addresses, email addresses, phone numbers, billing account numbers, and pricing plan details. Financial data, dates of birth, and government identification numbers were not compromised. The breach affects a critical infrastructure operator in the energy sector, creating regulatory notification obligations and elevated risk of targeted social engineering against the exposed customer base.

## Technical Analysis

London Hydro disclosed unauthorized access to customer account and personal information systems on June 20, 2026. The exposed dataset includes names, postal addresses, email addresses, phone numbers, billing account numbers, and pricing plan details. Financial records, dates of birth, and government IDs were confirmed out of scope. The attack vector and initial access method have not been disclosed publicly. No CVE is associated with this incident. Mapped CWE: CWE-284 (Improper Access Control), indicating a likely failure in authorization enforcement protecting customer data stores. MITRE ATT&CK techniques inferred from incident pattern analysis: T1005 (Data from Local System), T1078 (Valid Accounts), T1530 (Data from Cloud Storage Object). No threat actor has been attributed. The investigation is ongoing and no patch or remediation advisory has been published by the vendor.

## Action Checklist

1. Step 1: Containment, If your organization is a utility or critical infrastructure operator using similar customer information management systems, audit current access controls on customer PII stores immediately. Review NIST AC-3 (Access Enforcement) and AC-6 (Least Privilege) compliance: confirm that only authorized roles can query billing account and contact databases. Revoke any anomalous or unrecognized sessions active around June 20, 2026.
2. Step 2: Detection, Per NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs), query authentication and data access logs for bulk exports or abnormal read volumes against customer PII tables. Hunt for T1078 indicators: account logins outside business hours, service accounts accessing customer data stores, and lateral movement from internet-facing systems. Check cloud storage access logs for T1530 patterns (mass object enumeration or download from blob/bucket storage).
3. Step 3: Eradication, No vendor patch is available for this incident as it is not a software vulnerability. Remediation is procedural: enforce NIST AC-2 (Account Management) by auditing and disabling any accounts that accessed customer data without a documented business need. Apply NIST AC-2 (Account Management) controls to restrict data store access to named, role-specific accounts only. Rotate credentials for any service accounts with access to customer PII systems per NIST IA-5 (Authentication and Authorization).
4. Step 4: Recovery, Validate that access control lists on customer data systems are scoped to least privilege per CIS 3.3 (Configure Data Access Control Lists). Confirm logging is active and forwarding correctly per CIS 8.2. Monitor for secondary misuse of the exposed data set: watch for spear-phishing campaigns targeting London Hydro customers using billing account numbers as lure content. Run a tabletop to confirm your own incident response playbook covers third-party data breach notification workflows.
5. Step 5: Post-Incident, This incident exposes a control gap in access governance for customer PII within operational technology-adjacent environments. Map gaps against NIST AC-2 (Account Management), AC-6 (Least Privilege), and AU-12 (Audit Record Generation). If your organization operates customer-facing billing or account systems, conduct a data inventory review per CIS 3.2 (Establish and Maintain a Data Inventory) and verify retention and disposal policies under CIS 3.4 and 3.5. Assess whether your supplier or peer-utility risk monitoring covers similar critical infrastructure operators.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | URGENT |
| **Escalation Criteria** | Escalate immediately to legal counsel and executive leadership if forensic analysis confirms bulk export of the 170,000-customer PII dataset from your own systems, if any financial account data or government identification numbers are found in scope contrary to initial assessment, or if Canadian PIPEDA breach-of-security-safeguards reporting obligations are triggered (real risk of significant harm to affected individuals). |

| | |
|---|---|
| **Recovery Notes** | Post-containment, maintain enhanced monitoring on customer billing database access logs and authentication systems for a minimum of 30 days, as threat actors who obtained billing account numbers and contact details may use this data to facilitate account takeover attempts or targeted phishing against both London Hydro customers and employees. Validate that all ACL changes and credential rotations applied during eradication are reflected in your authoritative IAM or database role documentation before returning systems to normal operational status. Monitor peer-utility threat sharing channels (e.g., E-ISAC for energy sector) for intelligence indicating the exposed dataset is being traded or exploited in secondary campaigns. |
| **Forensic Artifacts** | Database audit logs (pgaudit SELECT events or MySQL General Query Log) for June 19–21, 2026, showing row counts, authenticated usernames, source IPs, and exact column names queried against customer PII tables — the primary artifact for establishing exfiltration volume and actor identity \| Application-layer API or web server access logs (/var/log/apache2/access.log, /var/log/nginx/access.log, or IIS logs) for endpoints serving customer account data, filtered for bulk pagination patterns (e.g., repeated requests with incrementing offset parameters or high response-body sizes) indicating systematic data harvesting \| Authentication logs (Linux /var/log/auth.log or Windows Security Event Log Event IDs 4624, 4625, 4648, 4776) on billing application and database hosts, capturing the source IP, account name, logon type, and timestamp for all sessions active in the June 19–21, 2026 window \| Cloud storage access logs (AWS CloudTrail S3 data events or Azure Blob Storage diagnostic logs) if customer data was stored in or staged to object storage, showing ListBucket and GetObject API calls with requester identity, object keys, and byte counts — critical for establishing whether data was exfiltrated via cloud egress \| Network flow records (NetFlow, VPC Flow Logs, or firewall session logs) for the database host subnet covering June 19–21, 2026, showing outbound connection volumes and destination IPs from database servers — anomalous outbound data volume to non-whitelisted external IPs is a key indicator of exfiltration staging |

## Per-Action IR Details

**Step 1: Containment — If your organization is a utility or critical infrastructure operator using similar customer information management systems, audit current access controls on customer PII stores immediately. Review NIST AC-3 (Access Enforcement) and AC-6 (Least Privilege) compliance: confirm that only authorized roles can query billing account and contact databases. Revoke any anomalous or unrecognized sessions active around June 20, 2026.**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.3 — Containment Strategy

**Controls:** NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AC-12 (Session Termination)

**Compensating:** Without enterprise PAM tooling, run 'SELECT usename, application_name, client_addr, state, query_start FROM pg_stat_activity;' (PostgreSQL) or 'SELECT session_user, host, db, command, time FROM information_schema.processlist;' (MySQL) to enumerate live sessions on customer billing databases. Export and diff against your authorized service account list. Kill unauthorized sessions with 'SELECT pg_terminate_backend(pid);' or 'KILL CONNECTION id;'. For Windows-based billing systems, run 'query session /server:' and 'Get-CimInstance Win32_LogonSession' to enumerate active sessions before termination.

**Evidence:** Before revoking any sessions: capture 'pg_stat_activity' or MySQL 'processlist' output showing active connections to customer PII tables, including client IP, username, query text, and session start time. Export database audit logs (e.g., PostgreSQL pgaudit logs at /var/log/postgresql/, or MySQL General Query Log) covering June 19–21, 2026, focusing on SELECT statements against customer name, postal address, email, phone, billing account number, and pricing plan columns. Snapshot active OS-level network connections via 'netstat -ano' or 'ss -tulnp' on database hosts before session termination. These volatile artifacts will be destroyed upon session revocation.

**Step 2: Detection — Per NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs), query authentication and data access logs for bulk exports or abnormal read volumes against customer PII tables. Hunt for T1078 indicators: account logins outside business hours, service accounts accessing customer data stores, and lateral movement from internet-facing systems. Check cloud storage access logs for T1530 patterns (mass object enumeration or download from blob/bucket storage).**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2 — Detection and Analysis

**Controls:** NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

**Compensating:** Without SIEM, use grep or awk against pgaudit or MySQL General Query Log to identify rows-returned counts exceeding normal thresholds: 'grep -E "AUDIT.*SELECT" /var/log/postgresql/postgresql-*.log | awk -F"rows=" \'NR>1 && $2+0 > 500 {print}\'' . For authentication anomalies on Linux billing hosts, run 'last -a | grep -v "still logged in" | awk \'$7 !~ /^(09|10|11|12|13|14|15|16|17)/ {print}\'' to surface off-hours logins. For AWS S3 or Azure Blob, export CloudTrail/Activity Logs and filter for 'ListBucket' or 'GetObject' events with request counts >1000 in a single session using AWS CLI: 'aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventName,AttributeValue=GetObject --start-time 2026-06-19 --end-time 2026-06-21'.

**Evidence:** Collect before any containment action alters log state: database audit trail records (pgaudit SELECT events with row counts, timestamps, source IP, and authenticated user) for June 19–21, 2026; application-layer web/API server access logs (Apache/Nginx /var/log/apache2/access.log or /var/log/nginx/access.log) filtered for endpoints serving customer account data; authentication logs (/var/log/auth.log or Windows Security Event Log Event ID 4624/4625/4648) on systems with access to billing databases; and cloud storage access logs (AWS CloudTrail S3 data events or Azure Blob Storage diagnostic logs) showing object enumeration or bulk download activity targeting customer data buckets.

**Step 3: Eradication — No vendor patch is available for this incident as it is not a software vulnerability. Remediation is procedural: enforce NIST AC-2 (Account Management) by auditing and disabling any accounts that accessed customer data without a documented business need. Apply D3-UAP (User Account Permissions) controls to restrict data store access to named, role-specific accounts only. Rotate credentials for any service accounts with access to customer PII systems per D3-CRO (Credential Rotation).**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication

**Controls:** NIST AC-2 (Account Management), NIST AC-6 (Least Privilege)

**Compensating:** Without enterprise IAM tooling, enumerate all database accounts and role grants via 'SELECT grantee, table_name, privilege_type FROM information_schema.role_table_grants WHERE table_schema = \'customer_data\';' (PostgreSQL) and cross-reference against HR-provided authorized role list. Disable unauthorized accounts with 'ALTER USER NOLOGIN;' (PostgreSQL) or 'REVOKE ALL ON customer_data.* FROM \'\'@\'%\';' (MySQL). For service account credential rotation, update connection strings in application config files (e.g., /etc/billing-app/db.conf) and restart services; document each change with timestamp and authorizing analyst in a change log.

**Evidence:** Before disabling accounts or rotating credentials: capture the full output of 'SELECT usename, usesuper, usecreatedb, usecreaterole, valuntil FROM pg_user;' and 'SELECT * FROM information_schema.role_table_grants WHERE table_schema = \'customer_data\';' to establish a pre-eradication account baseline. Export the complete database audit log covering the breach window (June 19–21, 2026) showing every account that executed SELECT against PII columns (name, email, phone, postal_address, billing_account_number, pricing_plan). Capture service account last-login timestamps and source IPs from authentication logs before credential rotation destroys session continuity evidence.

**Step 4: Recovery — Validate that access control lists on customer data systems are scoped to least privilege per CIS 3.3 (Configure Data Access Control Lists). Confirm logging is active and forwarding correctly per CIS 8.2. Monitor for secondary misuse of the exposed data set: watch for spear-phishing campaigns targeting**

**London Hydro customers using billing account numbers as lure content. Run a tabletop to confirm your own incident response playbook covers third-party data breach notification workflows.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** CIS 3.3 (Configure Data Access Control Lists), CIS 8.2 (Collect Audit Logs), NIST AU-6 (Audit Record Review, Analysis, and Reporting)

**Compensating:** Validate ACLs without enterprise tooling by running 'SHOW GRANTS FOR \'\'@\'\';' for each database role and comparing against a documented least-privilege matrix. Verify log forwarding by injecting a known test SELECT against a canary row in the customer table and confirming the event appears in the central log destination within 60 seconds. For phishing monitoring with no commercial threat intel feed, configure a free Google Alert for 'London Hydro' combined with 'billing' or 'account' to surface public phishing kit references, and monitor abuse.ch URLhaus for newly submitted URLs containing 'londonhydro' as a domain substring.

**Evidence:** At recovery stage, volatile evidence should already be preserved from prior phases. Confirm that log forwarding continuity is verified by reviewing log ingestion timestamps — a gap in pgaudit or auth.log forwarding around June 20, 2026 is itself a forensic artifact indicating potential log tampering or exfiltration staging. Monitor email gateway logs and DNS query logs for domains spoofing London Hydro (e.g., typosquat domains like 'londonhydro-billing[.]ca') as indicators that the exposed billing account numbers are being weaponized in downstream phishing campaigns.

**Step 5: Post-Incident — This incident exposes a control gap in access governance for customer PII within operational technology-adjacent environments. Map gaps against NIST AC-2 (Account Management), AC-6 (Least Privilege), and AU-12 (Audit Record Generation). If your organization operates customer-facing billing or account systems, conduct a data inventory review per CIS 3.2 (Establish and Maintain a Data Inventory) and verify retention and disposal policies under CIS 3.4 and 3.5. Assess whether your supplier or peer-utility risk monitoring covers similar critical infrastructure operators.**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity

**Controls:** NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST AU-12 (Audit Record Generation), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 3.4 (Enforce Data Retention), CIS 3.5 (Securely Dispose of Data)

**Compensating:** Conduct the data inventory review using a structured spreadsheet mapping each customer PII field (name, postal address, email, phone, billing account number, pricing plan) to its storage location, access roles, retention period, and disposal method — achievable by a 2-person team in a half-day workshop. For AU-12 gap assessment without SIEM, verify that pgaudit or MySQL General Query Log is enabled and capturing DML/DDL by running 'SHOW VARIABLES LIKE \'general_log\'' and 'SELECT * FROM pg_settings WHERE name = \'pgaudit.log\'' and confirming output includes 'READ' or 'ALL' event classes.

**Evidence:** Post-incident evidence collection focuses on lessons-learned documentation rather than volatile artifacts. Preserve: the complete database audit log from the breach window as an immutable artifact (hash with SHA-256 and store offline); the pre- and post-eradication account permission snapshots for audit trail continuity; any gap analysis outputs from the AC-2/AC-6/AU-12 control review; and the data inventory spreadsheet identifying which PII fields were stored, where, and with what access controls at the time of the breach. This evidence package supports both internal lessons-learned review and any regulatory notification obligations under Canadian privacy law (PIPEDA breach-of-security-safeguards reporting requirements).

## Detection Guidance

No IOCs have been publicly released for this incident. Detection should focus on behavioral and access anomalies consistent with the mapped ATT&CK techniques. For T1078 (Valid Accounts): review authentication logs for logins from unusual geolocations or IP ranges, after-hours access to customer databases, and service

accounts performing interactive logins. For T1005 (Data from Local System): alert on bulk file reads or exports from systems hosting customer PII, especially where the volume significantly exceeds baseline. For T1530 (Data from Cloud Storage): if customer data resides in cloud object storage, enable and review access logs for mass LIST or GET operations, particularly from principals not part of normal application workflows. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) cadence: review relevant logs at least weekly, or trigger automated alerting on threshold-based anomalies. No specific event IDs, signatures, or hashes are available from published sources at this time.

## Framework Mappings

### MITRE-ATTACK

- **T1005** — Data from Local System
- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage

### NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement

### OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

### CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

### SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents
- **CC6.3** — Authorizes, modifies, or removes access

### HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

### ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

### NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1005 | Data from Local System | Collection |
| T1078 | Valid Accounts | Defense-Evasion |
| T1530 | Data from Cloud Storage | Collection |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Canadian Electricity Provider London Hydro Discloses Data Breach** | https://www.securityweek.com/canadian-electricity-provider-london-h... | T3 |
| **Canadian utility fesses up to data breach, but key details remain off ...** | https://www.theregister.com/security/2026/06/22/canadian-utility-fe... | T3 |
| **Canadian Electricity Provider London Hydro Discloses Data Breach** | https://www.linkedin.com/posts/angelo-caproitti-b72532211_canadian-... | T3 |
| **Canadian Electricity Provider London Hydro Discloses Data Breach** | https://securityboulevard.com/2026/06/canadian-electricity-provider... | T3 |
| **Canadian Electricity Provider London Hydro Discloses Data Breach** | https://www.show.it/canadian-electricity-provider-london-hydro-disc... | T3 |



Generated 2026-06-24 19:00 UTC by TJS Security Command Center