INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-12 15:46 UTC

Kyushu Electric Loses External Drive Containing 10.9 Million Customer Records in Physical Security Failure

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0166
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Kyushu Electric Power Co. (subsidiary), internal backup infrastructure; unspecified external storage device (SSD/removable drive) containing customer personal data
Published	2026-06-11T19:14:16
Discovery Source	Rss

Executive Summary

A subsidiary of Kyushu Electric Power Co. lost an external storage drive containing personal data for up to 10.9 million customers, roughly the entire population of the Kyushu region, after the device went missing from an unlocked server room cabinet on May 26, 2026. The drive held customer personal information collected through an informal backup process that operated outside standard storage controls, and its encryption status has not been confirmed publicly. The primary business risks are regulatory exposure under Japan's Act on Protection of Personal Information, reputational damage at regional scale, and potential downstream fraud or social engineering targeting affected customers.

Technical Analysis

This incident is a physical security and data governance failure, not a network intrusion. Affected infrastructure: a Kyushu Electric subsidiary's internal backup environment using removable external storage media (reported as SSD). No CVE applies. Relevant CWEs: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor), CWE-311 (Missing Encryption of Sensitive Data), CWE-284 (Improper Access Control), CWE-693 (Protection Mechanism Failure). The drive was stored in an unlocked cabinet in a server room, indicating a physical access control gap. The backup procedure was ad hoc and outside normal capacity controls, a process governance failure. MITRE ATT&CK techniques consistent with the scenario: T1052 (Exfiltration Over Physical Medium), T1052.001 (Exfiltration over USB/removable media), T1078 (Valid Accounts, insider threat vector, unconfirmed). Encryption status of the drive is unconfirmed; if unencrypted, all 10.9 million records are

presumed fully exposed. Financial login credentials and payment card numbers were not reported as part of the exposed data in available sources, though confirmation of full contents is pending. Attribution is unknown, insider threat or physical intruder remain equally plausible. No patch exists; remediation is procedural and physical.

Action Checklist

1. Step 1: Containment, Audit all removable media currently in use across backup infrastructure. Identify any additional unencrypted drives holding customer or sensitive data. Physically secure or remove them from unlocked storage immediately. Reference: CIS 3.6 (Encrypt Data on End-User Devices) applied to removable backup media.
2. Step 2: Detection, Review physical access logs for the server room where the drive was stored, covering the 30-day window prior to May 26, 2026. Correlate badge or keycard access records with shift schedules. Check CCTV or entry logs if available. Query asset management systems (CIS 1.1, Establish and Maintain Detailed Enterprise Asset Inventory) for removable media check-out/check-in records. Look for any anomalous after-hours access events (NIST SI-4, System Monitoring, applied to physical monitoring logs).
3. Step 3: Eradication, Terminate the ad hoc backup procedure that produced the unsecured drive. Replace with an approved, encrypted, and auditable backup process. Enforce full-disk encryption on all removable media containing personal data (CIS 3.6). Revoke physical access credentials for any unresolved access anomalies identified in Step 2 (CIS 6.2, Establish an Access Revoking Process). Apply NIST AC-2 (Account Management) and AC-3 (Access Enforcement) to server room access controls.
4. Step 4: Recovery, Validate that no additional unauthorized copies of the customer dataset exist on removable media, cloud staging areas, or personal devices. Confirm all remaining backup media is encrypted and inventoried. Restore server room physical security to a locked, access-controlled state. Notify affected customers per APPI obligations and engage Japan's Personal Information Protection Commission as required. Document incident timeline per NIST IR-5 (Incident Monitoring) and IR-6 (Incident Reporting).
5. Step 5: Post-Incident, Conduct a formal lessons-learned review under NIST IR-4 (Incident Handling). Specific control gaps exposed: absence of removable media encryption policy (CWE-311), failure of physical access controls on media storage (CWE-284), no formal approval process for ad hoc backup procedures (CWE-693), and inadequate asset inventory for removable media (CIS 1.1). Establish mandatory encryption for all backup media (CIS 3.6), restrict removable storage use to approved procedures only (CIS 2.3, Address Unauthorized Software, applied to unauthorized media), and require quarterly physical security audits of server room access logs (NIST AU-6, Audit Record Review, Analysis, and Reporting).

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to executive leadership, legal counsel, and Japan's Personal Information Protection Commission if forensic review of physical access logs or CCTV footage identifies a specific individual who removed the drive (converting potential loss to confirmed theft), if any portion of the 10.9 million customer records appears on dark web marketplaces or paste sites, or if investigation reveals the ad hoc backup procedure produced additional unaccounted-for copies of the dataset.
Recovery Notes	Recovery cannot be declared complete until the data inventory confirms all copies of the 10.9 million customer record dataset are either physically secured and encrypted or formally destroyed per CIS 3.5 (Securely Dispose of Data). Monitor dark web and open-source intelligence sources (e.g., HaveIBeenPwned, Japanese-language paste sites, underground forums) for the appearance of Kyushu Electric customer data — specifically name, address, contract number, and usage data fields — for a minimum of 90 days post-incident. APPI requires ongoing notification obligations if new evidence of data misuse emerges after the initial filing, so the incident record must remain open and monitored until the 90-day window closes without evidence of exposure.
Forensic Artifacts	Physical access control system logs for the specific server room cabinet — badge/keycard reader event records covering April 26 – May 26, 2026, including entry timestamps, credential IDs, and any failed or overridden access attempts | CCTV footage from server room entrance and cabinet area for the same 30-day window — highest volatility artifact, typically on a 30-day overwrite cycle; must be exported to write-once media within hours of incident declaration | Asset management system or manual media register records for the missing external storage device — including serial number, label, last check-out date, last custody holder, and any check-out/check-in transaction history | Backup job logs and scheduling records for the ad hoc backup procedure that wrote the customer dataset to the missing drive — including the operator account that initiated the job, the timestamp, the data source path, and the destination device identifier | IT change management, email, or ticketing system records authorizing or acknowledging the ad hoc backup procedure — these establish the chain of human decisions that bypassed standard storage controls and are critical for root-cause attribution and regulatory reporting

Per-Action IR Details

Step 1: Containment — Audit all removable media currently in use across backup infrastructure. Identify any additional unencrypted drives holding customer or sensitive data. Physically secure or remove them from unlocked storage immediately. Reference: CIS 3.6 (Encrypt Data on End-User Devices) applied to removable backup media.

NIST Phase: Containment

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

Controls: CIS 3.6 (IG1/IG2/IG3) — Encrypt Data on End-User Devices, CIS 1.1 (IG1/IG2/IG3) — Establish and Maintain Detailed Enterprise Asset Inventory, NIST AC-19 — Access Control For Mobile Devices

Compensating: Use a spreadsheet-based manual media register if no asset management system exists: assign two staff members to physically walk all server rooms and backup staging areas, record each drive's serial number, label, encryption status (verify via BitLocker status command 'manage-bde -status' on Windows or 'cryptsetup status' on Linux), and current cabinet/rack location. Photograph each drive and its storage location for the incident record. For drives whose encryption status is unknown, treat as unencrypted until confirmed otherwise.

Evidence: Before physically relocating or securing any drive, document its exact storage location (cabinet number, rack unit, room), photograph the unlocked cabinet where the missing drive was last held, and capture the asset management system's last check-in/check-out record for every removable drive in the affected server room. Record the serial numbers and labels of all drives present. This preserves the physical crime scene state before containment actions alter it — critical for insurance, regulatory, and law enforcement purposes under the APPI breach investigation.

Step 2: Detection — Review physical access logs for the server room where the drive was stored, covering the 30-day window prior to May 26, 2026. Correlate badge or keycard access records with shift schedules. Check CCTV or entry logs if available. Query asset management systems (CIS 1.1 — Establish and Maintain Detailed Enterprise Asset Inventory) for removable media check-out/check-in records. Look for any anomalous after-hours access events (NIST SI-4 — System Monitoring, applied to physical monitoring logs).

NIST Phase: Detection Analysis

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

Controls: CIS 1.1 (IG1/IG2/IG3) — Establish and Maintain Detailed Enterprise Asset Inventory, NIST AU-6 — Audit Record Review, Analysis, And Reporting, NIST AU-3 — Content Of Audit Records

Compensating: If no electronic badge access system exists, interview all personnel with keys or physical access to the server room cabinet and document responses in writing with timestamps. Export CCTV footage (if present) to a write-once medium immediately — many CCTV systems overwrite on a 30-day cycle, meaning footage from May 26, 2026 may be at imminent risk of overwrite. For the media check-out register, pull any paper logs, email authorizations, or ticketing system entries referencing the missing drive's serial number or label. Cross-reference HR shift schedules against all documented access events using a simple timeline spreadsheet.

Evidence: Immediately preserve: (1) badge/keycard access logs for the specific server room from April 26 – May 26, 2026, exported to a read-only format before any log rotation occurs; (2) all available CCTV footage covering the server room entrance and cabinet area for the same window — this is the most volatile artifact and may overwrite within days; (3) the asset management or manual register entry for the missing drive, including last recorded custody holder and date; (4) any IT ticketing, email, or change management records referencing the ad hoc backup procedure that created the drive. None of these can be reconstructed after overwrite or system changes.

Step 3: Eradication — Terminate the ad hoc backup procedure that produced the unsecured drive. Replace with an approved, encrypted, and auditable backup process. Enforce full-disk encryption on all removable media containing personal data (CIS 3.6). Revoke physical access credentials for any unresolved access anomalies identified in Step 2 (CIS 6.2 — Establish an Access Revoking Process). Apply D3-UAP (User Account Permissions) and D3-CH (Credential Hardening) to server room access controls.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 3.6 (IG1/IG2/IG3) — Encrypt Data on End-User Devices, CIS 6.2 (IG1/IG2/IG3) — Establish an Access Revoking Process, CIS 4.6 (IG1/IG2/IG3) — Securely Manage Enterprise Assets and Software, NIST AC-2 — Account Management, NIST AC-3 — Access Enforcement

Compensating: To terminate the ad hoc backup procedure immediately without a replacement system in place: issue a written directive to all backup operators suspending removable media use, collect all drives currently checked out, and store them in a locked cabinet with dual-key access. For credential revocation of anomalous access holders, submit deprovisioning requests to the physical security team and building management within 24 hours of identification — document each revocation with timestamp, requester, and approver. Use BitLocker (Windows) or VeraCrypt (cross-platform, free) to encrypt any newly authorized replacement media before first use.

Evidence: Before revoking physical access credentials or terminating backup operator access, capture and preserve: (1) a complete list of all individuals whose badge credentials currently permit server room entry, with access grant dates and authorizing manager; (2) the specific access log entries flagged as anomalous in Step 2, exported and hashed for evidentiary integrity; (3) any documentation of who authorized or was aware of the ad hoc backup procedure, including email chains, verbal authorization records, or change tickets. Revoking credentials before preserving this attribution chain may impede the root-cause investigation and any subsequent HR or legal action.

Step 4: Recovery — Validate that no additional unauthorized copies of the customer dataset exist on removable media, cloud staging areas, or personal devices. Confirm all remaining backup media is encrypted and inventoried. Restore server room physical security to a locked, access-controlled state. Notify affected customers per APPI obligations and engage Japan's Personal Information Protection Commission as

required. Document incident timeline per NIST IR-5 (Incident Monitoring) and IR-6 (Incident Reporting).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 3.2 (IG1/IG2/IG3) — Establish and Maintain a Data Inventory, CIS 3.4 (IG1/IG2/IG3) — Enforce Data Retention, CIS 1.1 (IG1/IG2/IG3) — Establish and Maintain Detailed Enterprise Asset Inventory, NIST AU-11 — Audit Record Retention, NIST AC-3 — Access Enforcement

Compensating: For cloud staging validation without enterprise DLP: query cloud storage accounts (AWS S3, Azure Blob, Google Drive, etc.) accessible to backup operators for any bucket or folder containing files with naming conventions or sizes consistent with the customer dataset. For personal device review, issue a written attestation request to all backup personnel asking them to confirm no copies of the dataset exist on personal devices — retain signed attestations. Use 'dir /s' (Windows) or 'find' (Linux) to scan authorized backup servers for files matching the dataset's expected size range and modification date of May 26, 2026 or earlier.

Evidence: Before declaring recovery complete, verify and document: (1) written confirmation from the data owner that the full scope of the 10.9 million customer records dataset has been mapped and all known copies are accounted for; (2) encryption verification output (BitLocker status or equivalent) for every remaining removable drive in the backup inventory; (3) the completed APPI breach notification filing and timestamp of submission to the Personal Information Protection Commission — regulatory notification is a required recovery milestone, not a post-incident task; (4) updated server room access control configuration showing the cabinet is now locked and access is restricted to named, authorized personnel only.

Step 5: Post-Incident — Conduct a formal lessons-learned review under NIST IR-4 (Incident Handling). Specific control gaps exposed: absence of removable media encryption policy (CWE-311), failure of physical access controls on media storage (CWE-284), no formal approval process for ad hoc backup procedures (CWE-693), and inadequate asset inventory for removable media (CIS 1.1). Establish mandatory encryption for all backup media (CIS 3.6), restrict removable storage use to authorized procedures only (CIS 2.3 — Address Unauthorized Software, applied to unauthorized media), and require quarterly physical security audits of server room access logs (NIST AU-6 — Audit Record Review, Analysis, and Reporting).

NIST Phase: Post Incident

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

Controls: NIST AU-6 — Audit Record Review, Analysis, And Reporting, CIS 1.1 (IG1/IG2/IG3) — Establish and Maintain Detailed Enterprise Asset Inventory, CIS 3.6 (IG1/IG2/IG3) — Encrypt Data on End-User Devices, CIS 2.3 (IG1/IG2/IG3) — Address Unauthorized Software, CIS 7.1 (IG1/IG2/IG3) — Establish and Maintain a Vulnerability Management Process, NIST AU-2 — Event Logging

Compensating: For a resource-constrained team, conduct the lessons-learned review as a structured 90-minute tabletop with all backup operators, the server room custodian, and IT management present — use the documented incident timeline as the agenda anchor. Produce three required outputs: (1) a written removable media policy prohibiting ad hoc backup procedures without change management approval; (2) a quarterly physical audit checklist covering server room lock status, cabinet access logs, and removable media inventory reconciliation; (3) a mandatory encryption standard requiring BitLocker or VeraCrypt on all removable media before customer data is written. File all outputs with the APPI compliance record for this incident.

Detection Guidance

Physical security detection: Pull server room badge/keycard access logs for the 30 days preceding May 26, 2026. Flag any access events outside normal business hours or by personnel without documented need. Cross-reference with personnel schedules and visitor logs. If CCTV covers the server room, review footage for the same window. Asset and media tracking: Query asset management or IT ticketing systems for removable media check-out records. Identify whether the missing drive appears in any formal inventory (CIS 1.1). Absence

from inventory itself is a finding. Audit log review: Review any system or application logs that recorded data transfers to removable media in the backup environment (NIST AU-2, Event Logging; NIST AU-12, Audit Record Generation). Data exfiltration behavioral indicators: If endpoint DLP tools are deployed, search for large-volume file copy events to USB or external storage devices in the weeks before the discovery date (MITRE T1052.001). Insider threat indicators: Unusual access to customer data repositories, off-hours logins, or attempts to disable logging on backup servers (MITRE T1078, Valid Accounts). Note: encryption status of the drive remains unconfirmed as of the time of this report. If forensic recovery of the drive occurs, priority verification should establish whether AES-256 or equivalent full-disk encryption was applied.

Framework Mappings

MITRE-ATTACK

- **T0895** — Autorun Image
- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage
- **T1052.001** — Exfiltration over USB
- **T1052** — Exfiltration Over Physical Medium

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-13** — Cryptographic Protection

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting
- **164.312(e)(1)** — Transmission Security

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T0895	Autorun Image	Execution
T1078	Valid Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection
T1052.001	Exfiltration over USB	Exfiltration
T1052	Exfiltration Over Physical Medium	Exfiltration

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/japanese-energy-firm...	T3
Massive data breach feared at Kyushu Power as SSD missing	https://www.asahi.com/ajw/articles/16629979	T3
Kyushu Electric Power Subsidiary Reports Potential Theft of SSD ...	https://beyondmachines.net/event_details/kyushu-electric-power-subs...	T3
Kyushu Electric lost backup drive containing data of 10.9 million clients	https://cyberinsider.com/kyushu-electric-lost-backup-drive-containi...	T3
Kyushu power company loses hard drive containing 11 million ...	https://www.reddit.com/r/japan/comments/1u0t19g/kyushu_power_compan...	T3

Generated 2026-06-12 15:46 UTC by TJS Security Command Center