INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:40 UTC

Data Breach at Harvard’s Development Office May Have Exposed Donor Records, Personal Information

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0009
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Harvard University Alumni Affairs and Development Office information systems; alumni, donor, student, and faculty records
Published	Nov 22, 2025

Executive Summary

An unauthorized party accessed Harvard University's Alumni Affairs and Development Office systems, exposing personal contact information, donation records, and event data belonging to alumni, donors, students, and faculty. The breach was discovered in November 2025; stolen data including email and home addresses has since been confirmed published online (per TechRadar reporting), increasing risk of downstream social engineering campaigns. Organizations that share donor or partnership data with Harvard, and any institution relying on similar alumni management systems, should assess their own exposure and data-sharing agreements.

Technical Analysis

Initial access is reported as a vishing (voice phishing) attack targeting staff with access to alumni and development systems. Medium confidence assessment, sourced from secondary reporting rather than official Harvard disclosure. Once access was obtained, the attacker exfiltrated records from systems supporting the Alumni Affairs and Development Office. No CVE is associated with this incident; the attack chain maps to credential-based compromise rather than a software vulnerability. Relevant CWEs: CWE-287 (Improper Authentication), CWE-359 (Exposure of Private Personal Information to Unauthorized Actor). MITRE ATT&CK techniques: T1589.002 (Gather Victim Identity Information: Email Addresses), T1078 (Valid Accounts, likely used post-vishing to authenticate), T1566.004 (Phishing: Spearphishing Voice), T1530 (Data from Cloud Storage), T1567 (Exfiltration Over Web Service). No patch is applicable; this is an access control and social engineering failure. Law enforcement has been notified. No threat actor has been publicly attributed. Stolen data

confirmed leaked online per TechRadar reporting.

Action Checklist

1. Step 1, Immediate: Audit any data-sharing agreements or integrations with Harvard's Alumni Affairs and Development Office systems; determine whether your organization's data was within scope of the exposed records.
2. Step 2, Detection: Review inbound call logs and helpdesk ticket history for social engineering attempts targeting staff with access to CRM, donor management, or alumni platforms; look for account access anomalies in those systems from November 2025 onward.
3. Step 3, Assessment: Inventory staff roles with access to constituent relationship management (CRM), fundraising, or event management systems; verify MFA enrollment and session token hygiene for those accounts.
4. Step 4, Communication: If your organization shares donor, alumni, or partner records with third-party institutions, notify your privacy and legal teams to assess notification obligations under applicable data protection regulations (FERPA, state breach notification laws).
5. Step 5, Long-term: Conduct vishing awareness training targeting staff in development, alumni relations, finance, and IT helpdesk roles; implement callback verification procedures for any request involving credential resets or system access grants made over the phone.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to external IR firm immediately if: (1) evidence of active attacker persistence detected in your CRM/development systems post-November 2025; (2) downstream social engineering attacks targeting your staff confirmed; or (3) your organization's donor/partner data is confirmed published in public breach databases.
Recovery Notes	After containment: (1) Force password reset for all CRM/development staff; (2) revoke and re-issue API tokens for Harvard integration; (3) implement 30-day intensive logging and alerting on all CRM/development system access (session creation, data export, user creation/deletion); (4) conduct forensic review of CRM database change logs to identify unauthorized data exfiltration (query: SELECT * FROM audit_log WHERE event_type='export' AND timestamp>='2025-11-01'). (5) Retain all forensic evidence for legal proceedings (threat: downstream litigation from affected alumni/donors under state breach notification laws).
Forensic Artifacts	Active Directory audit logs (Event ID 4720: user account created, 4722: account enabled, 4723: password change attempt) | CRM application database audit tables (login events, data export queries, credential changes, schema modifications post-Nov 2025) | VPN/MFA gateway authentication logs (failed and successful login attempts, MFA enrollment events) | Helpdesk ticketing system (all tickets containing keywords: 'password', 'reset', 'access', 'credential', 'Harvard' from Nov 2025 onward) | Email gateway logs and message tracking (phishing attempts, credential-harvesting domains, sender reputation analysis for spoofed institutional addresses)

Per-Action IR Details

Step 1, Immediate: Audit any data-sharing agreements or integrations with Harvard's Alumni Affairs and Development Office systems; determine whether your organization's data was within scope of the exposed records.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: understanding your environment and assets)

Controls: NIST 800-53 IA-4 (Identifier Management), NIST 800-53 SA-9 (External Information System Services), CIS 6.1 (Establish and maintain a data management process)

Compensating: Query your contract management system or shared drives for all agreements naming Harvard as a third party. Cross-reference API integration documentation in your network diagram or systems inventory spreadsheet. If no formal inventory exists, interview CRM/development operations leads and document findings in a spreadsheet with columns: system name, data classification, fields shared, integration method (API/SFTP/manual), last sync date.

Evidence: Capture before auditing: (1) Full text of all active data-sharing agreements with Harvard (PDF/email); (2) Screenshots of API authentication tokens or integration configuration in your CRM system; (3) Database schema documentation showing which tables/fields sync to/from Harvard; (4) IT change log entries for integrations created/modified between 2024–2025. Store in isolated, read-only archive.

Step 2, Detection: Review inbound call logs and helpdesk ticket history for social engineering attempts targeting staff with access to CRM, donor management, or alumni platforms; look for account access anomalies in those systems from November 2025 onward.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.4 (Detection and Analysis: using monitoring and log review to identify indicators of compromise)

Controls: NIST 800-53 AU-2 (Audit Events), NIST 800-53 SI-4 (Information System Monitoring), CIS 8.8 (Implement User Activity Logging)

Compensating: If no SIEM exists, export helpdesk tickets and call center logs to CSV. Filter by keywords: 'password reset', 'account unlock', 'urgent', 'verify credentials', 'confirm email', targeting staff in development/fundraising departments. Cross-reference against CRM access logs (export from your system's audit trail or database query: SELECT * FROM audit_log WHERE event_type IN ('login', 'credential_change') AND user_department LIKE '%Development%' AND timestamp >= '2025-11-01'). Flag logins outside business hours or from new IP ranges. Document all anomalies in a timeline spreadsheet with columns: timestamp, user, system, event, severity.

Evidence: Capture immediately (before social engineering investigation begins): (1) Full helpdesk/ticketing system database export filtered to Nov 2025–present; (2) Call center CDR (call detail records) with phone numbers and caller context; (3) CRM/fundraising system audit logs (login, logout, password reset, data export events); (4) Firewall/proxy logs showing outbound connections from development staff workstations (filter by user account); (5) Email gateway logs for phishing/credential-harvesting attempts (search: Harvard, development, fundraising, password, verify). Preserve with hashing (SHA-256) for forensic integrity.

Step 3, Assessment: Inventory staff roles with access to constituent relationship management (CRM), fundraising, or event management systems; verify MFA enrollment and session token hygiene for those accounts.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.3 (Profiling normal network and system behavior to establish baselines); NIST 800-61r3 §4.2.2 (Eradication: removing the attacker's access)

Controls: NIST 800-53 IA-2 (Authentication), NIST 800-53 IA-5 (Authentication), NIST 800-53 IA-6 (Access Identifiers), CIS 5.2 (Use MFA for all access to administrative functions), CIS 5.3 (Disable Dormant Accounts)

Compensating: Query your Active Directory/identity provider for all users in groups matching 'Development', 'Fundraising', 'CRM_Admins', 'Alumni_Relations'. For each user, export: user ID, email, last login, MFA enrollment status (via AD Properties or identity management system). If MFA enrollment data is unavailable, query your VPN/2FA gateway logs (e.g., Duo, Okta, Microsoft Authenticator) for users who have not enrolled. Cross-reference with CRM system access logs to confirm functional access. Create a spreadsheet with remediation plan (enroll MFA, rotate

credentials, revoke stale sessions) and track completion. For session token hygiene, review CRM application settings for session timeout (target: 15–30 min inactivity) and force-logout on password change.

Evidence: Capture before remediation: (1) Active Directory user export with MFA status, last logon timestamp, group membership (output from AD query or PowerShell Get-ADUser); (2) CRM application access logs showing user login/logout and session duration (past 90 days); (3) VPN/MFA gateway authentication logs confirming MFA factors enrolled per user (past 30 days); (4) Screenshots of MFA configuration policy in your identity system; (5) Password change/reset logs for all flagged users (past 180 days). Store hashed or encrypted in secure archive for forensic reference.

Step 4, Communication: If your organization shares donor, alumni, or partner records with third-party institutions, notify your privacy and legal teams to assess notification obligations under applicable data protection regulations (FERPA, state breach notification laws).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §6 (Post-Incident Activities: lessons learned, notification, disclosure); NIST 800-53 IR-6 (Incident Reporting)

Controls: NIST 800-53 IR-6 (Incident Reporting), NIST 800-53 IR-8 (Incident Response Planning), CIS 6.5 (Requirement for Data Handling and Transmission)

Compensating: Coordinate with Legal and Privacy officers (no tool dependency). Document: (1) A list of all data types shared with Harvard (names, emails, donation amounts, addresses); (2) State-by-state applicability (California's CCPA, New York's SHIELD Act, etc.); (3) FERPA applicability if your org is education-adjacent or has student records; (4) Notification timeline requirements per each applicable law (typically 30–60 days). Create a notification matrix with rows = affected states, columns = law, notification requirement, timeline, responsible party. Brief C-level and external counsel before any disclosure.

Step 5, Long-term: Conduct vishing awareness training targeting staff in development, alumni relations, finance, and IT helpdesk roles; implement callback verification procedures for any request involving credential resets or system access grants made over the phone.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §6 (Post-Incident Activities: improving defenses and implementing lessons learned); NIST 800-53 AT-2 (Security Awareness and Training)

Controls: NIST 800-53 AT-2 (Security Awareness and Training), NIST 800-53 AT-3 (Role-Based Security Training), NIST 800-53 IA-2 (Authentication), CIS 14.2 (Security Awareness and Training Program)

Compensating: Partner with HR to roll out mandatory vishing training (free options: NIST Cybersecurity Framework awareness modules, CISA phishing simulation toolkits). Implement callback verification via written procedure: (1) Any phone request for credential reset or access grant → helpdesk agent notifies requestor that callback will be made to official company directory number; (2) Helpdesk agent hangs up, independently verifies caller's identity (check directory, call official number), then calls back; (3) Document callback verification in ticket system. Provide quick reference cards to helpdesk and finance staff with approved escalation paths (e.g., 'Always call [CIO name] directly if the request sounds urgent or comes from unfamiliar number').

Detection Guidance

No confirmed IOCs have been published from this incident. Detection focus should be behavioral. In your own environment: (1) Review authentication logs for CRM and donor management platforms, flag logins from new devices, unusual geolocations, or off-hours access. (2) Check helpdesk and call logs for social engineering patterns: requests to reset credentials, bypass MFA, or grant access made verbally without written follow-up. (3) If Harvard's systems included cloud storage integration (as suggested by T1530 mapping), monitor for bulk download events or exports to personal or external accounts. Note: Cloud storage involvement has not been confirmed by official sources. (4) Monitor for your organization's data appearing in breach aggregator feeds or

paste sites. The Harvard data has already been published online, increasing the likelihood it will be used in follow-on phishing or spearphishing campaigns targeting the exposed individuals. Treat affected email and home address data as actively exploitable for downstream social engineering.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.techradar.com/pro/security/personal-data-stolen-during-harvard-and-upenn-data-breaches-leaked-online-emails-home-addresses-and-more-all-published`	TechRadar reporting confirming stolen data published online, human validation recommended; URL sourced from item data, not independently verified	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1589.002** — Email Addresses
- **T1078** — Valid Accounts
- **T1567** — Exfiltration Over Web Service
- **T1566.004** — Spearphishing Voice
- **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
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3**
- **6.4**
- **6.5**
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

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

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training
- **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
T1589.002	Email Addresses	Reconnaissance
T1078	Valid Accounts	Defense-Evasion
T1567	Exfiltration Over Web Service	Exfiltration
T1566.004	Spearphishing Voice	Initial-Access
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
Thecrimson	https://www.thecrimson.com/article/2025/11/22/alumni-affairs-data-b...	T3
Harvard University database hacked; alumni, donors, students, and ...	https://timesofindia.indiatimes.com/technology/tech-news/harvard-da...	T3
Unauthorized access to Harvard alumni databases via phone phishing	https://www.linkedin.com/posts/ekiledjian_harvard-reports-data-brea...	T3
Personal data stolen during Harvard and UPenn data breaches ...	https://www.techradar.com/pro/security/personal-data-stolen-during-...	T3

Source	URL	Tier
Harvard cyberattack data breach exposes alumni, donors, students ...	https://m.economictimes.com/news/international/us/harvard-cyberatta...	**T3**

Generated 2026-03-29 18:40 UTC by TJS Security Command Center