INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-15 06:01 UTC

University of Nottingham Hacked, Over 450,000 Students Affected

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0173
Type	Data Breach
Severity	HIGH
Affected Products	University of Nottingham, student and former student records (450,000+ individuals)
Published	2026-06-14
Discovery Source	Gemini

Executive Summary

The University of Nottingham has confirmed a cyberattack in which threat actors gained unauthorized access to and exfiltrated personal data belonging to more than 450,000 current and former students; the data was subsequently leaked publicly. The breach affects a large population of individuals whose records were held by the university, creating immediate notification obligations and sustained reputational exposure. While the specific attack vector remains undisclosed, the confirmed public leak elevates regulatory and litigation risk significantly.

Technical Analysis

The University of Nottingham confirmed unauthorized access to and exfiltration of student records affecting 450,000+ individuals. As of the analysis date, the specific initial access vector, exploited vulnerability, and full data taxonomy have not been publicly disclosed. No CVE identifier or CWE classification has been issued because the breach does not stem from a disclosed software vulnerability. Investigation is ongoing to determine root cause. MITRE ATT&CK techniques mapped by the upstream pipeline are T1078 (Valid Accounts), T1530 (Data from Cloud Storage), and T1566 (Phishing), indicating the breach likely involved credential-based or social engineering initial access followed by cloud storage exfiltration. No threat actor has been attributed. Breach occurrence confidence is HIGH, corroborated by Have I Been Pwned and SecurityWeek. Root cause confidence is LOW; technical details are not yet publicly available.

Action Checklist

1. Containment: If your institution uses shared identity federation or cross-institutional access with the University of Nottingham, immediately audit and suspend any active federated sessions or trust relationships. Review NIST AC-17 (Remote Access) controls to ensure federated sessions are properly terminated and trust relationships are revoked where not mission-critical.

2. Detection: Query identity provider logs for anomalous authentication events consistent with T1078 (Valid Accounts): logins from unfamiliar geolocations, off-hours access, and bulk data access patterns. For T1530, review cloud storage access logs for large-scale object enumeration or download events. Enable alerting per NIST AU-6 (Audit Record Review, Analysis, and Reporting). CIS 8.2 (Collect Audit Logs) should be verified as active across all systems holding student PII.

3. Eradication: If you operate systems storing student or alumni PII, enforce credential rotation per NIST IA-4 (Credential Management) for all accounts with access to those systems. Disable any dormant or unreviewed accounts per CIS 5.3 (Disable Dormant Accounts). Conduct a review of cloud storage bucket permissions against CIS 3.3 (Configure Data Access Control Lists) to confirm no unintended public or over-permissioned access exists.

4. Recovery: Validate that multi-factor authentication is enforced on all externally exposed applications and administrative interfaces per CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.5 (Require MFA for Administrative Access). Verify audit logging continuity per NIST AU-4 (Audit Storage Capacity) and AU-11 (Audit Record Retention). Confirm no unauthorized accounts or persistence mechanisms remain in identity systems using NIST AC-2 (Account Management).

5. Post-Incident: Conduct a data inventory review per CIS 3.2 (Establish and Maintain a Data Inventory) to identify all systems holding student or alumni PII and assess whether access controls are calibrated to need-to-know. Review separation of duties per NIST AC-5 to ensure no single account can enumerate and exfiltrate large datasets without triggering an alert. Update incident response playbooks to address cloud storage exfiltration scenarios mapped to T1530.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to institutional data protection officer, legal counsel, and executive leadership if your systems share identity federation with the University of Nottingham, if evidence of lateral data access to your own student PII repositories is detected, or if your institution holds records of any of the 450,000+ affected individuals — triggering UK GDPR Article 33 72-hour notification obligations to the ICO and potential Article 34 communication requirements to affected data subjects.
Recovery Notes	After containment, restore student-data systems to production only after completing a full account audit confirming no unauthorized accounts, OAuth grants, or scheduled tasks persist, and after verifying MFA enforcement is active on all externally exposed interfaces. Monitor IdP authentication logs and cloud storage access logs continuously for a minimum of 30 days post-recovery for re-entry attempts using credentials potentially harvested from the Nottingham breach and circulated on threat actor forums. Given that the breached data was publicly leaked, credential-stuffing campaigns targeting other UK higher-education institutions using Nottingham student email addresses should be treated as an elevated and sustained threat for at least 90 days.

Forensic Artifacts	Identity provider authentication logs (Azure AD Sign-in logs / Shibboleth access logs): capture the full retention window immediately — look for logins using Nottingham-affiliated email domains or from IP ranges associated with the breach actor, particularly in the 30–90 days prior to public disclosure. | Cloud storage access logs (AWS CloudTrail data events for S3 GetObject/ListObjects, or Azure Blob Storage diagnostic logs for GetBlob/ListBlobs): these reveal whether bulk enumeration or download of student PII records occurred and are the primary artifact for quantifying exfiltration scope. | Student information system (SIS) application access logs: web server or application-tier logs for the SIS (e.g., Banner, Ellucian, PeopleSoft) showing unusually large query result sets, sequential record retrieval by student ID, or export-function invocations outside normal business hours. | Active Directory event logs (Event ID 4624 — Logon, 4648 — Explicit Credential Use, 4720 — Account Created, 4732 — Member Added to Security Group): capture from domain controllers covering the estimated breach window to identify credential misuse or persistence account creation targeting systems with student PII access. | Email and file-sharing platform audit logs (Microsoft 365 Unified Audit Log or Google Workspace Admin Audit): search for bulk download or forwarding of student records files, external sharing events on PII-containing documents, and any OAuth application consent grants that could facilitate persistent data access.

Per-Action IR Details

Containment — If your institution uses shared identity federation or cross-institutional access with the University of Nottingham, immediately audit and suspend any active federated sessions or trust relationships. Review NIST AC-17 (Remote Access) controls for externally connected systems handling student or staff PII.

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-12 (Session Termination), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export and review SAML/OIDC federation trust metadata from your IdP (Azure AD: `Get-MsolFederationProperty`; Shibboleth: review `relying-party.xml`). Enumerate active cross-institutional trust relationships manually and document each before disabling. Use PowerShell `Get-AzureADServicePrincipal` or equivalent to identify federated app registrations tied to Nottingham domains.

Evidence: Before suspending federated sessions, capture: active SAML assertion logs from your IdP showing any sessions originating from Nottingham-affiliated identity providers (look for issuer URIs containing `nottingham.ac.uk`); OAuth token issuance logs showing cross-institutional delegated permissions; current active session tokens from your student information system or shared research portals. These are volatile — token state and active session bindings are lost on revocation.

Detection — Query identity provider logs for anomalous authentication events consistent with T1078 (Valid Accounts): logins from unfamiliar geolocations, off-hours access, and bulk data access patterns. For T1530, review cloud storage access logs for large-scale object enumeration or download events. Enable alerting per NIST AU-6 (Audit Record Review, Analysis, and Reporting). CIS 8.2 (Collect Audit Logs) should be verified as active across all systems holding student PII.

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-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: For cloud storage enumeration without SIEM: AWS — `aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventName,AttributeValue=ListObjects` filtered to your student-data buckets; Azure Blob — query Storage Diagnostic Logs for `GetBlob` or `ListBlobs` operations at abnormal volume. For IdP log review without SIEM: export Azure AD Sign-in logs to CSV and parse with PowerShell for `ResultType -ne 0` (failures) or

`LocationDetails` showing unexpected countries. Sigma rule `proc_creation_win_net_use_susp_mount` can catch lateral access attempts on Windows systems hosting PII.

Evidence: This step is analytical and does not alter live state. Preserve before analysis: IdP sign-in log snapshots (Azure AD: export from Entra portal covering 90-day retention window before it rolls); cloud storage access logs (AWS S3 server access logs or CloudTrail data events — note CloudTrail data-plane logging may not be enabled by default and must be checked immediately); any WAF or reverse-proxy access logs for the student records portal showing unusually large HTTP GET response sizes or sequential record ID enumeration patterns consistent with bulk data harvesting.

Eradication — If you operate systems storing student or alumni PII, enforce credential rotation for all accounts with access to those systems per D3-CRO (Credential Rotation). Disable any dormant or unreviewed accounts per CIS 5.3 (Disable Dormant Accounts). Conduct a review of cloud storage bucket permissions against CIS 3.3 (Configure Data Access Control Lists) to confirm no unintended public or over-permissioned access exists.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 5.3 (Disable Dormant Accounts), CIS 3.3 (Configure Data Access Control Lists), NIST AC-2 (Account Management), NIST AC-6 (Least Privilege)

Compensating: Credential rotation without PAM tooling: generate a privileged account list from Active Directory using `Get-ADUser -Filter {Enabled -eq $true} -Properties LastLogonDate | Where-Object {$_.LastLogonDate -lt (Get-Date).AddDays(-45)}` to identify dormant accounts for immediate disablement. For cloud bucket ACL review: AWS `aws s3api get-bucket-acl --bucket ` and `aws s3api get-bucket-policy` for each bucket containing PII; flag any `Principal: *` entries as critical misconfigurations. Azure equivalent: `az storage container show-permission` for each container.

Evidence: Before rotating credentials or disabling accounts, capture: a full export of current account privilege assignments and last-logon timestamps from Active Directory or your IdP (this baseline is destroyed when accounts are modified); cloud IAM role and policy bindings as-is (AWS: `aws iam get-account-authorization-details`; Azure: `az role assignment list`); any existing cloud storage access logs not yet exported — log retention windows may expire during a prolonged response. Credential rotation on a compromised account without prior log capture eliminates the audit trail of what that account accessed.

Recovery — Validate that multi-factor authentication is enforced on all externally exposed applications and administrative interfaces per CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.5 (Require MFA for Administrative Access). Verify audit logging continuity per NIST AU-4 (Audit Storage Capacity) and AU-11 (Audit Record Retention). Confirm no unauthorized accounts or persistence mechanisms remain in identity systems using D3-LAM (Local Account Monitoring).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), NIST AU-4 (Audit Storage Capacity), NIST AU-11 (Audit Record Retention), NIST AC-2 (Account Management)

Compensating: MFA enforcement audit without enterprise tooling: enumerate all externally exposed applications from DNS records and your web application inventory; for each, verify MFA conditional access policy is applied (Azure AD: `Get-AzureADMSConditionalAccessPolicy`). For local account persistence check on Windows systems hosting student PII: `Get-LocalGroupMember -Group Administrators` and `Get-ScheduledTask | Where-Object {$_.TaskPath -notlike '\Microsoft\*'}` to detect backdoored scheduled tasks. For Linux/cloud: review `/etc/passwd` modifications and `~/.ssh/authorized_keys` on any host with PII access.

Evidence: Before declaring recovery and restoring production student data systems to full access, verify: no new accounts were created in the window between the estimated breach date and containment (Active Directory event log Event ID 4720 — User Account Created); no unauthorized OAuth application grants remain in the IdP (Azure: `Get-AzureADServicePrincipal | Get-AzureADServicePrincipalOAuth2PermissionGrant`); audit log storage capacity

and retention configuration to confirm logs covering the breach window have not been overwritten or purged — this is critical for regulatory notification and potential legal proceedings.

Post-Incident — Conduct a data inventory review per CIS 3.2 (Establish and Maintain a Data Inventory) to identify all systems holding student or alumni PII and assess whether access controls are calibrated to need-to-know. Review separation of duties per NIST AC-5 to ensure no single account can enumerate and exfiltrate large datasets without triggering an alert. Update incident response playbooks to address cloud storage exfiltration scenarios mapped to T1530.

NIST Phase: Post Incident

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

Controls: CIS 3.2 (Establish and Maintain a Data Inventory), NIST AC-5 (Separation Of Duties), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Data inventory without a commercial DLP tool: run `find / -name '*.csv' -o -name '*.sql' -o -name '*.xlsx'` on Linux file servers; use Windows `Get-ChildItem -Recurse -Include *.csv,*.xls,*.mdb` scoped to shares with student data. Tag findings against your student information system's data schema to identify shadow copies of PII outside authorized repositories. For bulk-exfiltration alerting without SIEM: configure AWS CloudWatch metric filter on `GetObject` API calls exceeding a per-hour threshold and trigger SNS notification; for on-prem, deploy a Sigma rule detecting Windows Event ID 4663 (Object Access) with high-frequency object read counts on PII file paths.

Evidence: Post-incident artifact preservation for lessons learned and regulatory reporting: preserve complete IdP authentication logs covering 90 days pre-detection and through containment; cloud storage access logs (with timestamps) showing the enumeration and exfiltration window; a snapshot of the data inventory state at breach time (reconstructed from backup or versioned configuration) to document exactly which student records were in scope; any threat actor TTPs identified during analysis mapped to the MITRE ATT&CK framework for playbook updates. These artifacts support UK GDPR Article 33 breach notification to the ICO and any subject access requests from affected individuals.

Detection Guidance

No confirmed IOCs are available in current source material. Detection should focus on behavioral indicators consistent with the mapped ATT&CK techniques. For T1078 (Valid Accounts): monitor identity provider and SSO logs for authentication from new geolocations, credential stuffing patterns (high-volume failed logins followed by success), and accounts accessing student record systems outside business hours. For T1530 (Data from Cloud Storage): alert on bulk object listing or download events in cloud storage platforms (S3, Azure Blob, Google Cloud Storage) from accounts that do not normally perform such operations. For T1566 (Phishing): review email gateway logs for credential harvest link clicks and correlate with subsequent authentication events. Apply NIST AU-6 review cadence to identity and cloud storage logs. Use file integrity monitoring to monitor authentication database changes. No specific event IDs, hashes, IPs, or domains are available from source material; do not substitute inferred IOCs.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage
- **T1566** — Phishing

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

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

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
University of Nottingham Data Breach - Have I Been Pwned	https://haveibeenpwned.com/Breach/UniversityOfNottingham	T3
University of Nottingham Confirms Breach After Hackers Leak Data	https://www.securityweek.com/university-of-nottingham-confirms-brea...	T3
Nottingham University data breach affects over 450000 students	https://www.reddit.com/r/technology/comments/1u3bvab/nottingham_uni...	T3

Source	URL	Tier
Nottingham International Law and Security Centre	https://www.nottingham.ac.uk/research/groups/nottingham-internation...	T3
day vulnerabilities and older security flaws to breach more than 100 ...	https://www.facebook.com/thescorpsec/posts/-the-university-of-notti...	T3

Generated 2026-06-15 06:01 UTC by TJS Security Command Center