INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-10 07:25 UTC

United Natural Foods (UNFI) Discloses Cyberattack Impacting Quarterly Earnings

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0156
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	United Natural Foods, Inc. (UNFI), enterprise IT systems
Published	2026-06-09
Discovery Source	Sec 8K

Executive Summary

United Natural Foods, Inc. (UNFI) disclosed a cyberattack via SEC 8-K filing on June 9, 2026, confirming the incident had a material financial impact on Q3 fiscal 2026 results, with net sales declining 4.2% to $7.7 billion for the 13-week period ended May 2, 2026. The attack type, initial access vector, affected systems, and scope of any data compromise have not been publicly disclosed. UNFI's operational disruption carries supply chain implications for downstream grocery retailers dependent on its distribution network.

Technical Analysis

UNFI disclosed a cybersecurity incident affecting enterprise IT systems via SEC 8-K filing (CIK 1020859, filed June 9, 2026). No CVE or CWE identifiers apply, this is an operational enterprise incident, not a software vulnerability disclosure. The attack type (ransomware, data exfiltration, business disruption) has not been confirmed in available source material. Affected systems, initial access vector, persistence mechanisms, lateral movement scope, and data compromise details are undisclosed. No MITRE ATT&CK techniques have been attributed. Attribution is unknown. The material financial impact was confirmed in the Q3 FY2026 earnings release filed concurrently with the 8-K. Technical indicators of compromise are not publicly available at this time.

Action Checklist

1. Step 1: Situational Awareness, Review UNFI's SEC 8-K filing (CIK 1020859, June 9, 2026) and the Q3 FY2026 earnings release for any updated disclosures on attack type, affected systems, or data compromise scope. Monitor UNFI's investor relations page and SEC EDGAR for amended filings.

2. Step 2: Detection, If your organization has third-party data-sharing, EDI integrations, or API connections with UNFI systems, audit those connection logs immediately. Per NIST SI-4 (System Monitoring), review network traffic logs for anomalous outbound connections to UNFI-affiliated IP ranges. Per CIS 8.2 (Collect Audit Logs), confirm logging is enabled on all integration endpoints and data exchange systems. No specific IOCs are publicly available for this incident.

3. Step 3: Supply Chain Risk Assessment, Identify all business processes dependent on UNFI order management, fulfillment APIs, or shared logistics platforms. Per NIST IR-4 (Incident Handling), activate third-party incident response procedures if UNFI systems touch your environment. Disable or quarantine active integrations until UNFI confirms system integrity.

4. Step 4: Recovery Posture, If UNFI integration services are suspended or degraded, validate that your own systems were not affected by any data exchange that occurred prior to the incident disclosure. Per NIST AU-6 (Audit Record Review, Analysis, and Reporting), review audit logs from integration points covering the period prior to the June 9, 2026 disclosure date. Per CIS 7.1 (Establish and Maintain a Vulnerability Management Process), assess whether shared credentials or tokens used for UNFI integrations require rotation.

5. Step 5: Post-Incident Control Review, Use this disclosure to evaluate third-party and supply chain risk management gaps. Per NIST IR-8 (Incident Response Plan), verify your IRP includes procedures for material vendor incidents disclosed via SEC filings. Per NIST IA-4 (Credential Management), rotate shared credentials and API tokens used for UNFI integrations. Per NIST SA-9 (External Information System Services), maintain and review your third-party dependency inventory to prioritize critical vendor relationships.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if forensic review of integration logs (Step 4) reveals that personal data, financial records, or proprietary business data transited UNFI systems during the confirmed compromise window, as this may trigger breach notification obligations under applicable state privacy laws or SEC cybersecurity disclosure rules (17 CFR 229.106).
Recovery Notes	Before restoring any UNFI EDI, API, or logistics integrations, obtain written confirmation from UNFI that affected systems have been restored and independently verified — do not rely solely on UNFI's public statements given the material financial impact and undisclosed attack scope. Monitor all restored integration endpoints for a minimum of 30 days post-reconnection, with daily review of connection volume and authentication anomalies against the pre-incident baseline. Given that UNFI's Q3 FY2026 disruption covers a 13-week window ending May 2, 2026, any data exchanged during that full quarter should be treated as potentially affected until UNFI provides a definitive scope statement in an amended SEC filing or direct vendor communication.

Forensic Artifacts	EDI/AS2 gateway transaction logs (February 1 – June 9, 2026): Preserved transaction-level records showing session initiator, authentication identity, byte volumes transferred, and UNFI endpoint hostnames — anomalous outbound volume spikes or sessions initiated outside normal batch windows are the primary indicator of potential data exposure during UNFI's compromise window. | API gateway access logs for UNFI-connected endpoints: Request/response logs including HTTP method, URI path, response code, payload size, and authentication token used — a pattern of unusually large GET responses or 200-OK replies to queries not initiated by your systems would suggest UNFI-side data was pushed to your environment while under attacker control. | Windows Security Event Log (Event IDs 4624, 4648, 4769, 5156) on integration servers: Logon and network connection events for the UNFI service account covering the exposure window — off-hours logons or source IPs inconsistent with your integration server's normal outbound NAT address indicate the credential may have been used outside your environment. | Firewall and perimeter netflow records (February 1 – June 9, 2026) filtered to UNFI IP ranges: Session duration, bytes sent/received, and protocol — an abrupt cessation of established sessions on or near the incident date confirms when UNFI systems went offline and brackets the exposure window; any sessions persisting after that point warrant immediate investigation as potentially attacker-controlled infrastructure. | Credential and secrets inventory audit trail: Configuration files, secrets managers, or vaulted entries containing UNFI API keys, OAuth tokens, SFTP credentials, or shared certificates — document each credential's creation date, last rotation date, and scope of access to confirm whether a compromised UNFI system could have harvested valid credentials that provide inbound access to your own environment.

Per-Action IR Details

Step 1: Situational Awareness — Review UNFI's SEC 8-K filing (CIK 1020859, June 9, 2026) and the Q3 FY2026 earnings release for any updated disclosures on attack type, affected systems, or data compromise scope. Monitor UNFI's investor relations page and SEC EDGAR for amended filings.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: Gathering initial indicators and scoping the incident from external disclosures prior to internal investigation

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives), NIST IR-6 (Incident Reporting)

Compensating: Set up a free SEC EDGAR RSS feed alert for UNFI CIK 1020859 (https://www.sec.gov/cgi-bin/browse-edgar?action=getcompany&CIK=1020859&type=8-K&dateb=&owner=include&count=10&search_text=) using a feed reader such as Feedly or a cron job calling the EDGAR API endpoint: `curl 'https://data.sec.gov/submissions/CIK0001020859.json' | python3 -m json.tool | grep -A5 '8-K'`. Assign one analyst to check daily until UNFI issues a follow-on filing or confirms system restoration.

Evidence: Before acting on secondary intelligence, capture a timestamped local copy of the June 9, 2026 8-K filing (SEC EDGAR accession number associated with CIK 1020859) as your threat-intelligence anchor document. Record any IP ranges, domain names, or system references mentioned in UNFI press releases or earnings call transcripts — these may later correlate to traffic visible in your own perimeter logs from the pre-disclosure window (approximately Q3 FY2026: February 1 – May 2, 2026).

Step 2: Detection — If your organization has third-party data-sharing, EDI integrations, or API connections with UNFI systems, audit those connection logs immediately. Per NIST SI-4 (System Monitoring), review network traffic logs for anomalous outbound connections to UNFI-affiliated IP ranges. Per CIS 8.2 (Collect Audit Logs), confirm logging is enabled on all integration endpoints and data exchange systems. No specific IOCs are publicly available for this incident.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: Correlating external vendor compromise signals against internal integration telemetry to assess lateral exposure

Controls: NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without SIEM: (1) Extract all EDI/API connection logs from your middleware or AS2/SFTP gateway for the period February 1 – June 9, 2026 and pipe through `grep` filtering on UNFI hostnames or IP ranges: `grep -E '(unfi\.com|)' /var/log/gateway/access.log > unfi_connections.txt`. (2) On Windows integration servers, query Windows Security Event Log for Event ID 4648 (explicit credential logon) and Event ID 5156 (Windows Filtering Platform permitted connection) filtered to UNFI destination IPs using: `Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4648,5156)} | Export-Csv unfi_auth_events.csv`. (3) Deploy Wireshark or `tcpdump -w unfi_capture.pcap host ` on integration nodes going forward to capture any resumed or anomalous session attempts.

Evidence: Capture and preserve before any changes: (1) Full AS2, SFTP, or EDI gateway transaction logs covering February 1 – June 9, 2026, including session initiation timestamps, authenticated user/service account identities, and byte-transfer volumes — abnormally large outbound transfers to UNFI endpoints during this window may indicate data staging or exfiltration. (2) NetFlow or firewall session logs showing connection frequency and volume to UNFI IP ranges — a sudden drop in established sessions around the incident date may mark when UNFI took systems offline. (3) API authentication tokens or OAuth credentials stored in integration middleware configuration files (e.g., `/etc/app/config.yml`, Windows Credential Manager, or `.env` files) — document their issuance dates and last-use timestamps before rotating.

Step 3: Supply Chain Risk Assessment — Identify all business processes dependent on UNFI order management, fulfillment APIs, or shared logistics platforms. Per NIST IR-4 (Incident Handling), activate third-party incident response procedures if UNFI systems touch your environment. Disable or quarantine active integrations until UNFI confirms system integrity.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment: Isolating third-party integration pathways as a containment boundary when the upstream vendor's system integrity cannot be confirmed

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: Without a formal TPRM platform: (1) Build a rapid dependency map using a spreadsheet — query your ERP or procurement system for all vendor IDs associated with UNFI (parent entity and subsidiaries) and cross-reference against active API keys, scheduled batch jobs, and SFTP accounts. (2) Disable scheduled EDI batch jobs immediately: on Linux, `crontab -l | grep unfi` and comment out relevant entries; on Windows, `Get-ScheduledTask | Where-Object {$_.TaskName -like '*UNFI*'} | Disable-ScheduledTask`. (3) Block UNFI IP ranges at the perimeter firewall with a documented temporary deny rule — log the rule with a review date tied to UNFI's restoration confirmation.

Evidence: Before disabling integrations, snapshot the current state: (1) Export all active firewall rules permitting traffic to/from UNFI IP ranges — this is your baseline to verify no unauthorized rules were inserted during the incident window. (2) Capture the process list and open network connections on integration servers using `netstat -antp | grep ` (Linux) or `netstat -ano | findstr ` (Windows) — an active session to a UNFI host after their disclosed outage may indicate a rogue or attacker-maintained channel. (3) Preserve copies of UNFI-specific API configuration files, including endpoint URLs, authentication headers, and certificate thumbprints, before any rotation — these document what credentials were in-scope during the exposure window.

Step 4: Recovery Posture — If UNFI integration services are suspended or degraded, validate that your own systems were not affected by any data exchange that occurred prior to the incident disclosure. Per NIST AU-6 (Audit Record Review, Analysis, and Reporting), review audit logs from integration points covering the period prior to the June 9, 2026 disclosure date. Per CIS 7.1 (Establish and Maintain a Vulnerability Management Process), assess whether shared credentials or tokens used for UNFI integrations require rotation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Verifying integrity of systems that exchanged data with the compromised vendor environment before restoring normal integration operations

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), NIST SI-2 (Flaw Remediation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For credential rotation without PAM tooling: (1) Identify all service accounts used exclusively for UNFI integrations by running `net user /domain | findstr svc` (Windows) or `grep unfi /etc/passwd` and reviewing application config files. (2) Rotate API tokens by generating new credentials in UNFI's partner portal (once restored) and updating local config files — use `find / -name '*.env' -o -name 'config.yml' 2>/dev/null | xargs grep -l 'UNFI'` to locate all credential references. (3) For audit log review, use `logparser` (free, Windows) or `awk` to filter integration logs by date range: `awk '$1 >= "2026-02-01" && $1 unfi_exposure_window.log` and review for data volume anomalies.

Evidence: Forensic review targets before restoring integrations: (1) Audit logs from your EDI/API gateway for the full Q3 FY2026 window (February 1 – May 2, 2026) — look for transfers to UNFI that are larger than historical baselines, which may indicate UNFI-side systems were staging or pulling data abnormally. (2) Authentication logs on your identity provider (Active Directory Security Event Log Event ID 4769 — Kerberos service ticket request, or Event ID 4624 — successful logon) for the UNFI integration service account — unexpected logon times or source IPs outside normal batch windows indicate potential credential misuse. (3) Integrity checksums of any data files received from UNFI during the exposure window — if UNFI's systems were compromised, inbound data could have been tampered with, affecting your own inventory or financial records.

Step 5: Post-Incident Control Review — Use this disclosure to evaluate third-party and supply chain risk management gaps. Per NIST IR-8 (Incident Response Plan), verify your IRP includes procedures for material vendor incidents disclosed via SEC filings. Per NIST SI-5 (Security Alerts, Advisories, and Directives), establish a monitoring process for 8-K cybersecurity disclosures from critical vendors. Apply D3-CRO (Credential Rotation) for any shared secrets with UNFI systems. Apply D3-ODM (Operational Dependency Mapping) to document and prioritize all critical third-party dependencies.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned, IRP updates, and supply chain control improvements driven by a material vendor cybersecurity disclosure

Controls: NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST IR-1 (Policy And Procedures), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Without a GRC platform: (1) Build a critical vendor watch list in a shared spreadsheet mapping vendor name, SEC CIK number (where applicable), primary integration type, data classification of exchanged data, and designated internal owner — update this with UNFI as a confirmed high-impact case. (2) Set up free SEC EDGAR EDGAR full-text search alerts via RSS for the term 'cybersecurity incident' filtered to your top 20 vendors by integration criticality. (3) Document the UNFI dependency map output from Step 3 as a formal third-party risk artifact — store alongside your IRP and schedule a quarterly review. For D3-ODM equivalent without tooling, use a simple RACI matrix mapping each UNFI-dependent business process to a system owner, data classification, and recovery time objective.

Evidence: Post-incident documentation to generate and retain: (1) A lessons-learned record specific to this event: what UNFI-facing controls existed before June 9, 2026, how quickly the integration was detected and contained, and what the credential rotation timeline was — this becomes your baseline for measuring improvement after the next third-party incident. (2) A written record of all UNFI-associated credentials rotated, including the service account name, rotation date, and approving authority — required to demonstrate NIST IR-4 (Incident Handling) compliance if audited. (3) Updated third-party risk register entry for UNFI documenting the incident date, SEC filing reference, business impact (supply chain disruption, 4.2% net sales decline disclosed in Q3 FY2026 earnings), and control gaps identified — this supports future vendor risk scoring and contract renegotiation.

Detection Guidance

No confirmed IOCs (IP addresses, domains, hashes, or behavioral signatures) have been publicly released for this incident. Organizations with direct system integrations with UNFI should: (1) Query firewall and proxy logs for anomalous traffic to UNFI-affiliated infrastructure during the weeks preceding June 9, 2026. (2) Review EDI transaction logs and API gateway logs for unusual data volumes, failed authentications, or unexpected session activity from UNFI-originated connections. (3) Per NIST AU-6, analyze audit records from data exchange points for indicators of unauthorized access or data staging. (4) Per CIS 8.2, confirm audit logging was active and intact on all integration endpoints, gaps in log continuity may themselves be an indicator. Until UNFI releases further technical details, detection must rely on anomaly analysis of integration traffic rather than signature-based methods. Monitor CISA and the SEC EDGAR filing system for updated disclosures.

Framework Mappings

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

NIST-800-53R5

- **CP-9** — System Backup
- **IR-4** — Incident Handling

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

Sources

Source	URL	Tier
SEC EDGAR Filing Index	https://www.sec.gov/Archives/edgar/data/1020859/000102085926000013/.. .	T1
(consolidated)	https://www.sec.gov/Archives/edgar/data/1020859/000102085926000013/.. .	T1
(consolidated)	https://www.sec.gov/Archives/edgar/data/763901/000119312526263044/0.. .	T1
(consolidated)	https://www.sec.gov/Archives/edgar/data/1559865/000155986526000039/.. .	T1

Source	URL	Tier
(consolidated)	https://www.sec.gov/Archives/edgar/data/1805284/000110465926071607/.. .	T1
United Natural Foods says cyberattack will reduce quarterly earnings	https://www.cybersecuritydive.com/news/unfi-cyberattack-reduce-quar...	T3

Generated 2026-06-10 07:25 UTC by TJS Security Command Center