



PUBLIC SAMPLE — FICTIONAL INCIDENT

All organizations, evidence, events, metrics and findings are invented. This is not an Acervus client engagement or a report on a real attack.

INCIDENT RESPONSE / POST-INCIDENT REVIEW

Cyber Incident Post-Mortem

Credential compromise and ransomware disruption

Example Distribution Group, Inc.

A fictional regional distribution business

Report identifier ACV-IR-PM-SAMPLE-001

Incident date 14 September 2026

Report date / version 18 September 2026 / 1.0

Reporting cutoff 18 September 2026, 17:00 UTC

Classification Public fictional sample; not confidential client material

Operational status Service restored; preventive work and data-impact review remain open

Intended readers Leadership, IT, security, operations and counsel

This example shows how an incident is reconstructed from evidence, how technical and organizational causes are distinguished, and how recovery is separated from long-term risk reduction.

Read with the limitations on page 8. Dates and action statuses are fixed to the reporting cutoff, not the date you download this sample.





01 / Executive summary

In this fictional scenario, an unauthorized party used a contractor remote-access account at 01:12 UTC on 14 September. The account was excluded from multi-factor authentication (MFA). A reused privileged credential and permissive administration paths allowed the session to reach internal systems. Ransomware activity began at 01:30, interrupting warehouse order processing.

Responders disabled the access path, revoked relevant sessions, isolated affected systems and rebuilt services from verified backups. Critical order processing returned at 09:45; the last affected business service was validated at 16:10. No ransom was paid in the scenario. The means by which the original credential was acquired and whether data left the environment remain unresolved.

Business impact — fictional estimates

Measure	Illustrative result and basis
Affected assets	23 workstations and 4 virtual servers encrypted: 27 of 86 inventoried assets (68 workstations, 18 servers).
Critical-service outage	8 hours 15 minutes, from 01:30 to 09:45 UTC.
Fulfillment delay	184 shipments queued; 142 released on 14 September and 42 on 15 September. No cancellations recorded in the simulated order ledger.
Direct response cost	\$51,500: response labor \$26,000; restoration services \$18,000; overtime \$7,500. Fictional estimates, not invoices.
Deferred order value	\$441,600 = 184 orders × \$2,400 average order value. Delayed gross order value, not lost revenue; not added to response cost.

Response intervals — one incident, not averages

Time to detection: 25 minutes from first observed unauthorized access (01:12) to the first alert (01:37); 7 minutes from observed encryption onset. **Alert to declaration:** 14 minutes. **Alert to containment milestone:** 41 minutes. **Alert to critical restoration:** 8 hours 8 minutes.

Severity is SEV-1 under this fictional organization's policy: loss of a critical business service requiring coordinated response. These timings are not MTTR or MTBD averages across incidents.



02 / Scope and evidence

The review covers identity, remote access, endpoint activity, warehouse systems, backups and restoration on 14 September, with supporting records from 1–18 September. “Confirmed” below means supported within the invented evidence set; nothing here represents a real forensic finding.

Reference	Synthetic evidence and what it supports
E-01 / Identity	VPN authentication and configuration exports: first observed access at 01:12; password-only exception for contractor-vpn-01. Does not establish how the password was obtained.
E-02 / Endpoint	Alert exports and collected event logs: encryption onset at 01:30, alert at 01:37, privileged activity and impacted-host sequence. Two affected servers lacked endpoint telemetry.
E-03 / Administration	Session and directory audit records: shared privileged credential used from the compromised access path. Correlation links sessions; it does not identify a person.
E-04 / Recovery	Offline backup inventory, restore job records and application tests: usable 00:00 UTC recovery point and validated service recovery.
E-05 / Business	Order queue reconciliation and operations signoffs: outage, delayed shipments and release dates.
E-06 / Network	Partial firewall and flow records. A collector interruption from 01:06–01:18 overlaps initial access and limits data-transfer assessment.

Findings and remaining uncertainty

High confidence within the scenario: unauthorized password-only access preceded privileged activity; ransomware encrypted the stated assets; backups enabled restoration. Supported by E-01 through E-05.

Moderate confidence: activity belongs to one connected access chain. Some host and network visibility is incomplete; alternative or earlier access cannot be excluded.

Unresolved: credential acquisition, actor identity, and data exfiltration. No conclusive evidence of exfiltration was recovered from the available records. That is not evidence that no data left.

A real engagement would retain originals, collection times, collector identities, cryptographic hashes, access history and custody transfers in a restricted evidence register. This public sample contains no real logs, indicators or evidence hashes.





03 / Reconstructed timeline

All times are UTC on 14 September 2026. Timestamps are exact within the fictional scenario, not a claim of perfect real-world clock accuracy.

UTC	Observed event or response decision	Basis
01:12	First observed unauthorized VPN authentication using the contractor account.	E-01
01:26	Privileged administration session correlated to the access path.	E-03
01:30	Encryption activity begins; warehouse order processing becomes unavailable.	E-02 / E-05
01:37	Endpoint alert reaches the on-call queue.	E-02
01:43	Analyst validates malicious activity and pages the incident commander.	Response log
01:51	SEV-1 declared. Command, evidence, recovery and communications roles assigned.	Decision log
02:02	Affected network segments and identified hosts isolated. Backup administration restricted.	Change record
02:18	Contractor account disabled; relevant sessions revoked; compromised administrative access blocked. Containment milestone, not proof of complete eradication.	E-01 / E-03
02:30	Leadership and counsel briefed; operations activates manual shipment triage.	Comms log
03:10	Clean recovery environment prepared; 00:00 backup selected and integrity checks begun.	E-04
05:40	Priority service rebuilds and credential changes complete; controlled restoration begins.	E-04
08:05	Warehouse application available to validators only; business testing starts.	Test record
09:45	Operations signs off critical order processing and authorizes staged return.	E-05
16:10	Final affected business service passes validation. Heightened monitoring continues.	E-04 / E-05

A configuration change that closes an entry path is not equivalent to confirming that all unauthorized persistence has been removed.



04 / Why the controls failed

The review is blameless: it examines control design, decision conditions and system behavior rather than assigning personal fault. This follows the review logic described by Atlassian and Rootly [1, 2].

Entry condition: password-only remote access

An MFA exception remained active after the contractor support window ended. It had no automatic expiry and no enforced recertification. E-01 establishes that the account accepted password-only access. The underlying credential-theft mechanism is unknown; this report does not label the event phishing without evidence.

Expansion condition: privileged access exceeded need

A shared administrative credential was accessible from the remote-access environment and reused across multiple systems. Network policy permitted administration paths outside the contractor's support scope. E-03 supports privileged use; the combination widened the potential impact of one account compromise.

Detection condition: uneven visibility

Two of four affected servers lacked active endpoint telemetry. Deployment exceptions were recorded but not linked to compensating controls. The central network collector's 12-minute interruption also reduced visibility into initial access. Neither gap independently explains the whole incident.

Causal chain

Unexpired MFA exception → unauthorized session → over-broad privileged and network access → encryption and disruption. Telemetry gaps limited detection and data-impact assessment; they are contributing factors, not substitutes for an entry-path explanation.

Why prior review did not reveal the exposure

The access review checked whether named accounts existed, not whether every live remote-access path enforced MFA. The recovery exercise tested backup readability, not an end-to-end warehouse restart after account revocation and credential rotation. Configuration state and business recovery therefore differed from the assumptions used in review.

Root-cause review should test assumptions against actual operating behavior. CrowdStrike's preliminary review and later RCA illustrate how deeper investigation can refine initial findings and map specific failure modes to mitigations [3, 4]. Their 2024 event was an update-related operational failure, not this fictional ransomware scenario.



05 / Response and restoration

Contain, preserve, rebuild, validate

Responders isolated identified systems and remote administration paths, preserved available logs and snapshots, disabled compromised access, revoked sessions and rotated exposed credentials. Restricting backup administration reduced the risk of modifying recovery material during the response.

Priority systems were rebuilt in a clean recovery environment rather than returning encrypted hosts directly to production. The 00:00 recovery point preceded first observed unauthorized access by 72 minutes; that timing alone did not prove it was clean. Restore integrity checks, malware screening and account review were required before business validation.

From 08:05 to 09:45, operations tested order ingestion, inventory reads, picking, label printing, shipment posting and reconciliation against the pre-outage ledger. The 90-minute difference between the recovery point and outage onset was treated as the potential transaction-reconstruction window. Missing transactions were reconciled from independent order records before release.

What worked

- Offline recovery material remained available and was validated before use.
- Early separation of command, evidence, recovery and communications roles reduced conflicting changes.
- Business owners signed off restoration; server startup alone was not treated as service recovery.

What did not work

- MFA and monitoring exceptions persisted without expiry or compensating controls.
- Shared privilege and broad network paths increased the reachable asset set.
- The recovery exercise had not rehearsed the complete dependency and credential-reset sequence.

Communications and residual risk

Leadership and counsel received the first consolidated briefing at 02:30. Scheduled updates distinguished known facts, open questions and next decisions. Operations contacted affected customers about fulfillment delays; those messages did not assert that no customer data had been accessed.

As of the reporting cutoff, restored services were operating without further observed encryption. This is a bounded observation, not proof of complete eradication. Data-impact review and legal notification decisions remained open.



06 / Corrective-action register

Statuses below are fictional and fixed as of 18 September. Completion requires evidence of effectiveness, not merely a ticket marked “done.” Due dates are in 2026.

Action / owner	Due / status	Required acceptance evidence
A-01 / Block compromised access Identity lead	14 Sep Implemented; initial test passed	Disabled-account test; session revocation log; rejection of the old privileged credential; retained test results.
A-02 / Enforce MFA on all remote-access paths Identity lead	22 Sep Open	Inventory of every path and exception; password-only access rejected; future exceptions auto-expire and have approval plus compensating controls.
A-03 / Replace shared administrative privilege Infrastructure lead	25 Sep Open	Named, least-privilege access; unique managed secrets; access logs attributable to a role/account; legacy shared secrets rejected.
A-04 / Limit vendor network reach Network lead	30 Sep Open	Authorized support paths succeed; unauthorized administrative and lateral paths fail in an observed segmentation test.
A-05 / Close telemetry gaps Security operations lead	23 Sep Open	Endpoint coverage reconciled to all 86 assets; unsupported assets isolated or compensated; simulated detection reaches on-call; collector-loss alert tested.
A-06 / Exercise full business recovery Operations + IT leads	30 Sep Open	Isolated restore drill includes credential resets, dependency startup and ledger reconciliation; measured critical-service recovery at or below the proposed 4-hour target.
A-07 / Resolve data-impact and notification review Counsel + investigation lead	21 Sep Open; statutory deadlines take precedence	Documented scope and evidence gaps; jurisdiction-specific notification decision and rationale; no unsupported “no breach” assertion.
A-08 / Verify preventive controls Executive risk owner	2 Oct Open	Review acceptance artifacts for A-02 through A-07; assign any residual risk explicitly; record independent challenge and next review date.

Closure gate: Service restoration does not close the corrective-action register. The incident commander documents the recovery basis; the executive risk owner accepts unresolved risks. The four-hour target is proposed, not an achieved result or a contractual SLA.





07 / Limitations and references

What this sample does — and does not — establish

This is original illustrative writing, not a reconstruction of a real incident, forensic evidence, client testimony or a finding about any named vendor. Names, dates, records, action owners and financial figures are fictional. Acervus did not investigate the fictional organization because no such engagement took place.

The simulated review is limited by incomplete endpoint coverage, a network-record gap and the possibility of activity before the review window. Restored availability is not evidence of no data access, no exfiltration or no persistence. Actor attribution and the means of credential acquisition remain unknown.

Real reports require scoped evidence collection, qualified investigation, restricted handling of personal and security-sensitive material, and review by counsel where appropriate. Notification obligations depend on facts, applicable law and contracts. Internal report deadlines never override a statutory or contractual deadline. This sample is not legal advice, an audit opinion or a guarantee against recurrence.

Methodological references

The following public sources informed the review structure and reasoning, not the invented incident facts. Referenced material was consulted on 12 October 2026. No affiliation, endorsement or vendor involvement is implied.

[1] Atlassian: Incident postmortems

Blameless review, clear timelines, impact and follow-through.

atlassian.com/incident-management/postmortem

[2] Rootly: Incident postmortems

Repeatable review, evidence, assigned owners and measurable actions.

rootly.com/incident-postmortems

[3] CrowdStrike: Preliminary post-incident review

24 July 2024; updated 25 July. Separating initial findings from a later investigation, and outlining prevention work.

crowdstrike.com — Falcon content update preliminary PIR

[4] CrowdStrike: Channel File 291 root cause analysis

6 August 2024. Explicit failure mechanisms, testing assumptions, findings paired with mitigations, and staged deployment.

crowdstrike.com — External Technical Root Cause Analysis, Channel File 291

Reference titles in this PDF are clickable. The CrowdStrike event was an operational disruption caused by a content update. Its technical findings and impacts are not attributed to the fictional organization in this sample.

