The Day the Network Disappeared

Cloud Control, Vendor Power, and Executive Accountability

Author: Jose Gabriel Guerrero Paredes

With expert support: Rogelio Ciau Chan

For classroom discussion. Details anonymized.

Publisher’s note

This document contains two versions of the same incident-based teaching case: (1) an MBA IT/technology risk version that goes deeper into architecture and recovery mechanics; (2) a CEO/Board version that focuses on enterprise risk, governance, and executive decision-making. Company and vendor identifiers have been anonymized. The protagonist is a recently appointed CIO.

Case Version: MBA - IT, Technology Risk, and Vendor Governance

Designed for MBA students and technology leaders. Includes enough technical detail to analyze failure modes, recovery options, and control design.

Synopsis

A recently appointed Chief Information Officer (CIO) at a large, asset-intensive services company inherits a newly opened headquarters network designed to operate almost entirely over Wi-Fi and managed through a cloud control plane. After an internet outage, an external network provider with administrative access removes or deletes the company's Central tenant/organization. Because no usable configuration backups exist, the headquarters network loses its configuration state and becomes inoperable. Operations dependent on headquarters connectivity are disrupted, forcing the CIO to coordinate crisis response, rapidly re-establish basic connectivity, and then rebuild the network configuration and governance model from scratch.

Learning objectives

- Diagnose how cloud-managed infrastructure can concentrate operational risk in a single control plane.
- Evaluate governance controls for third-party administrative access (identity, least privilege, auditability, termination).
- Design a pragmatic backup and recovery strategy for network configuration and management platforms.
- Lead executive communication and trade-off decisions during a high-visibility operational outage.
- Translate technical remediation into board-level risk reduction and investment decisions.

Primary dilemma

How should a newly appointed CIO establish control, resilience, and accountability when a critical operational environment is effectively controlled by external parties, lacks backups, and sits outside formal vendor governance?

Company context

- Industry: asset-intensive services (vehicle rental and related services).
- Scale: approximately USD 1-3B annual revenue; 3,000-5,000 employees.
- Footprint: a national network of ~195 operating locations plus two headquarters sites.
- Criticality: headquarters connectivity supported finance, call center operations, IT service management, and corporate functions; disruptions cascaded when WAN routing changed during an ISP event.

The CIO's starting position

Daniel Evans had been in the CIO role for roughly two months. Key vendor and network decisions had been made by a predecessor. The environment lacked several basic controls: formal vendor contracts for the headquarters network provider, defined SLAs, documented recovery procedures, and tested configuration backups.

Technical environment at headquarters

The headquarters building (approximately 500 workers) was designed with minimal wired connectivity. Most end-user access relied on Wi-Fi. Network management and configuration were centralized in Central (cloud control plane). The building did not have a dedicated firewall in the original design.

Connectivity and ISP setup

- Two ISP providers; seven internet services.
- One dedicated 100 Mbps symmetric service.
- Three 1 Gbps broadband services and three 500 Mbps business services.
- During the incident, traffic failed over to a backup backbone, changing which internet service was active.

Core network components (as documented post-incident)

- Cloud-managed gateway (Aruba 9012 class device) acting as the control point for the headquarters site.
- Multiple Aruba 6000 series switches (mix of 24-port, 48-port, and PoE variants) deployed across floors.
- Aruba 500-series access points (AP 505 class), approximately eight per floor.
- Server rooms on the first three floors feeding uplinks and distribution.

Vendor access and control plane dependency

Administrative access to Central was held by (a) the external provider that implemented the environment, (b) the CIO, and (c) the network/communications manager. Accounts were individual, but there was no independent audit process over privileged activity, and privileges available to internal staff were reported as limited.

Backup posture prior to the incident

- No usable configuration backups were found in Aruba Central.
- There was no separate offline export of VLANs, templates, or device profiles.
- No documented risk acceptance or formal recovery plan existed.

The incident

An external ISP outage triggers a network failover event. Daniel Evans contacted the external network provider to adjust which internet line the building was using (switching from one provider to another). Shortly afterward, the internal network team attempted to access Aruba Central and discovered the organization/tenant workspace was missing. Without the tenant, cloud-managed devices (switches and wireless infrastructure) lost synchronization and became effectively unmanaged.

What the audit later established

An independent operational report produced after the event concluded that the primary cause of the network collapse was the elimination or disassociation of the Aruba Central tenant/organization previously used to manage the devices. It also concluded there were no indicators of a cyberattack; the impact was consistent with deletion of the cloud environment combined with the absence of backups. The report stated that cloud-managed devices were left without configuration, without synchronization, and without remote management capability; recovery required rebuilding a new workspace and re-onboarding devices.

Operational impact

- Corporate finance systems and payment-related processes were disrupted; bookkeeping fell ~8 days behind.
- Call center operations and internal IT support were affected.
- Customer-facing cloud applications were largely unaffected, limiting direct revenue impact; the main quantified impact was late-payment penalties (~MXN 100k).

Timeline (approximate)

Time	Event	Decision pressure
Day 0 (AM)	ISP outage; network fails over to backup routing/backbone.	Restore basic connectivity; establish incident command.
Day 0 (Midday)	Provider engaged to switch active internet line.	Speed vs. control: who executes changes?
Day 0 (PM)	Aruba Central workspace/tenant found missing; devices lose cloud management.	Escalate to executives; choose recovery path.
Days 1-2	Emergency approach selected; a firewall is expedited and installed to restore critical connectivity.	Prioritize critical functions under uncertainty.
Days 3-10	Critical areas stabilized; phased rebuild continues.	Balance quick fixes with long-term redesign.
~2.5 weeks	Full stabilization and broader recovery; governance changes initiated.	Lock accountability model and vendor controls.

Decision points for classroom discussion

Decision 1: Recovery path when the control plane disappears

With the cloud tenant deleted and no configuration backup, CIO had to choose among imperfect recovery options:

- Rebuild Aruba Central workspace immediately and factory reset/re-adopt devices (high effort, slower initial recovery).
- Pivot to a temporary parallel network path (e.g., emergency firewall + segmentation) to restore critical operations first.
- Attempt vendor-driven restoration (risk: vendor leverage, unclear integrity, potential cost escalation).

Decision 2: Vendor containment and evidence preservation

The provider denied making changes and was slow to respond. CIO suspected the deletion could have been used to conceal other issues (for example, hardware warranty status). However, intent was not provable in the moment. What should CIO have done in the first 24-48 hours to protect the organization's legal and operational position?

Decision 3: Redesign versus stabilize

The incident exposed architectural weaknesses (near-total Wi-Fi dependence, unclear perimeter security, limited observability). CIO initiated changes, including moving critical workstations to wired Ethernet where

feasible and formalizing vendor governance. How should a CIO sequence redesign work while restoring service under pressure?

Exhibits

Exhibit 1: Observed control gaps

Control area	Observed gap	Why it mattered
Identity & access	External provider retained high privileges; activity not independently audited.	A single actor could remove the control plane without detection or immediate accountability.
Backup & recovery	No usable configuration backups in the management platform; no offline exports.	Deletion became a total loss event rather than a recoverable incident.
Vendor governance	No contract, no SLAs, no change control, limited escalation mechanisms.	No enforceable obligations or guardrails during crisis.
Asset assurance	Warranty/support coverage inconsistent; some devices could not be supported through vendor channels.	Slowed support and increased recovery cost and uncertainty.
Architecture resiliency	Headquarters heavily Wi-Fi dependent; limited perimeter architecture in the original design.	Reduced options for staged recovery and containment.

Exhibit 2: Minimum viable controls for cloud-managed network platforms

Students should evaluate which controls are preventive, detective, and corrective.

Control	Implementation pattern	Owner
Privileged access management	Named accounts, MFA, least privilege, time-bound elevation, break-glass procedures.	IT Security + Network Ops
Configuration backup	Scheduled exports of configs/templates; offline storage; quarterly restore tests.	Network Ops
Change management	Approval workflow for tenant-level actions; dual control for destructive operations.	IT Governance
Vendor access lifecycle	Access granted only per ticket; auto-expiry; offboarding checklist on vendor change.	Vendor Management
Monitoring & audit	Centralized logs for admin actions; alerts for tenant/org changes.	Security Operations

Discussion questions (MBA - IT)

1. From a risk-engineering perspective, what was the single most critical design flaw: the Wi-Fi-first architecture, lack of backups, vendor admin access, or lack of contracts? Defend your choice.

2. What recovery approach would you choose in the first 6 hours and why? What would you explicitly defer?
3. Design a control model for Aruba Central (or any cloud-managed platform) that prevents tenant deletion from becoming a catastrophic event. Include identity, backup, and approval controls.
4. Assume the vendor relationship is politically difficult to terminate. How do you reduce risk while keeping the vendor temporarily?
5. If you were the CIO, how would you communicate uncertainty to executives without losing credibility? Provide a 5-sentence executive update.

Case Version: CEO and Board - Enterprise Risk, Governance, and Crisis Leadership

Designed for CEOs, boards, and executive committees. Minimizes technical detail; emphasizes enterprise risk, accountability, and governance choices.

Synopsis

A recently appointed Chief Information Officer (CIO) at a large, asset-intensive services company inherits a newly opened headquarters network designed to operate almost entirely over Wi-Fi and managed through a cloud control plane (Aruba Central). After an internet outage, an external network provider with administrative access removes or deletes the company's Aruba Central tenant/organization. Because no usable configuration backups exist, the headquarters network loses its configuration state and becomes inoperable. Operations dependent on headquarters connectivity are disrupted, forcing the CIO to coordinate crisis response, rapidly re-establish basic connectivity, and then rebuild the network configuration and governance model from scratch.

Learning objectives

- Diagnose how cloud-managed infrastructure can concentrate operational risk in a single control plane.
- Evaluate governance controls for third-party administrative access (identity, least privilege, auditability, termination).
- Design a pragmatic backup and recovery strategy for network configuration and management platforms.
- Lead executive communication and trade-off decisions during a high-visibility operational outage.
- Translate technical remediation into board-level risk reduction and investment decisions.

Primary dilemma

How should a newly appointed CIO establish control, resilience, and accountability when a critical operational environment is effectively controlled by external parties, lacks backups, and sits outside formal vendor governance?

Company context

The company is a large, asset-intensive services business with USD 1-3B in annual revenue and 3,000-5,000 employees. Its headquarters houses approximately 500 corporate workers and supports finance, shared services, call center operations, and corporate IT. Many customer-facing systems run in the cloud, but day-to-day corporate operations depend on headquarters connectivity.

Why the outage mattered to executives

- Corporate finance and payment processes stalled; the company incurred late-payment penalties and accumulated operational backlog.
- Call center capacity and internal support were constrained, increasing operational risk during an already unstable event (ISP outage).
- The outage revealed that a third party could disrupt a critical environment without contractual obligations or oversight.

The inherited governance gap

Daniel Evans, a recently appointed CIO, inherited the headquarters network design and vendor setup. The environment had no formal contract with the network provider responsible for implementation and cloud administration; SLAs were undefined; escalation paths were informal. Critically, the company had no proven ability to restore network configuration if its cloud management environment was altered or removed.

The incident (executive view)

An ISP outage triggerd a failover event. During efforts to stabilize connectivity, the external provider with administrative access to the company's cloud-managed network environment removed or deleted the organization/tenant used to manage the headquarters network. With no usable backups, the headquarters network lost its configuration state and became inoperable.

What leadership knew and did not know

Known in first 24 hours	Unknown in first 24 hours
The cloud-managed environment was missing and the network was down.	Whether the deletion was accidental, negligent, or deliberate; and whether other configurations existed elsewhere.
Customer-facing cloud systems were largely intact.	Full operational dependency map and bandwidth/utilization metrics for headquarters.
Provider response was delayed and non-committal.	Whether hardware support/warranty status would hinder recovery.

The CIO's immediate actions

- Briefed the CEO and senior leadership on the operational impact and recovery path under uncertainty.
- Brought in an expedited emergency network/security component to restore basic connectivity to critical functions.
- Sequenced recovery to prioritize finance, treasury, and call center operations; non-essential staff temporarily shifted to remote work where feasible.

Audit conclusions (executive translation)

- Root cause: deletion/disassociation of the cloud-managed tenant/organization removed centralized configuration for network devices.
- No evidence of a cyberattack; failure mode consistent with administrative deletion combined with no backups.
- Recovery required rebuilding the management workspace and re-onboarding devices; some support paths were constrained by warranty/support coverage inconsistencies.

Board-level decision points

Decision 1: What is the enterprise's tolerance for vendor-administered control planes?

The incident demonstrated that a third party effectively controlled the headquarters network's configuration state. What controls must be mandatory for any vendor-administered system that can stop corporate operations?

Decision 2: Invest to reduce catastrophic single points of failure

Resilience is not free. The board must decide whether to fund a minimum viability package: configuration backups, privileged access controls, monitoring, and a tested recovery plan - even for infrastructure that appears 'commodity'.

Decision 3: Accountability model and operating cadence

Daniel Evans was accountable for the outage outcomes despite inheriting the design and vendor relationship. What governance cadence should the CEO and board require for critical operational technology risk (e.g., quarterly resilience reviews, vendor access audits, test results)?

Exhibits

Exhibit A: Board-ready control commitments (one-page)

Commitment	Board question	Evidence artifact
No destructive admin actions without dual control	Who can delete or disable a control plane?	Quarterly privileged access review + approval workflow evidence
Backups with restore testing	Can we rebuild in hours, not weeks?	Latest restore test report and RTO/RPO metrics
Vendor access lifecycle	Do vendors still have access after projects end?	Vendor access register + expiry logs
Incident playbook	Who runs command in the first hour?	Incident runbook and escalation tree
Architecture resilience roadmap	Where are our hidden single points of failure?	Top 10 operational dependency map + remediation plan

Discussion questions (CEO/Board)

6. What oversight should a board exercise over 'invisible' infrastructure risks that can still stop finance and corporate operations?
7. What minimum contractual and governance standards should apply to any vendor with privileged access to operationally critical systems?
8. In the first 24 hours, what would you expect from the CIO versus the CEO? Where should the decision rights sit?
9. If the company cannot fully insource network expertise, how should it structure managed services to avoid vendor lock-in and catastrophic access risk?
10. What would you fund immediately: backup/testing, privileged access management, network redesign, or vendor replacement? Justify the sequence.