NASCIO State IT Recognition Awards

No Ransom, Full Recovery: Nevada's Statewide Cyber Resilience Response

Cybersecurity

State	Nevada
Agency	Governor's Technology Office
Category	Cybersecurity
Project title	No Ransom, Full Recovery: Nevada's Statewide Cyber Resilience Response
Project dates	August 24, 2025 - October 28, 2025; hardening and monitoring ongoing
Contact	Michael Hanna-Butros Meyering, Chief Communications & Policy Officer | MichaelHBM@it.nv.gov

A statewide cyber incident became a real-world test of governance, continuity, recovery, and disciplined public communication.

Metric	Result
Statewide scope	60+ state agencies coordinated through a single recovery framework
Recovery speed	Business-critical services restored within 7 days; full-service recovery completed in 28 days
Fiscal discipline	No ransom paid; approx. 90% of impacted data recovered
Operational surge	4,212 overtime hours from 50 state employees; estimated $478,062 avoided vs. a contractor-only surge model

STATE OF NEVADA
GOVERNOR'S TECHNOLOGY OFFICE

Executive Summary

In August 2025, the State of Nevada faced a targeted ransomware event that disrupted statewide systems and tested the resilience of digital government. The Governor's Technology Office (GTO), under the leadership of the State CIO, executed an established incident response plan, escalated immediately to executive leadership, coordinated across more than 60 agencies, engaged trusted forensic, legal, recovery, and law enforcement partners, and prioritized services that Nevadans depend on: payroll, public safety, benefits eligibility, courts, emergency management, transportation, and essential agency operations.

The State made the strategic decision not to pay ransom. Instead, GTO used prepared playbooks, executive prioritization, specialized recovery teams, disciplined communication, and rapid hardening to contain the incident, restore business-critical services within the first week, complete full-service recovery in 28 days, and recover approximately 90% of impacted data. The remaining data was retained under state control and reviewed through a risk-based process.

The project is award-worthy because it shows cybersecurity as a public service discipline, not merely a technical function. Nevada demonstrated that investments in governance, cyber insurance, incident simulations, identity controls, vendor readiness, communications, and staff training can materially reduce harm when an incident occurs. The response protected taxpayer funds, preserved public confidence, and produced a stronger future-state roadmap for SOC maturity, endpoint detection and response, identity protection, training, and continuity of operations.

Submission Snapshot

Question	Answer
Category fit	Strengthens security and risk management posture through incident governance, assessment and audit, IAM hardening, data privacy review, business continuity, and disaster recovery.
Universal challenge	Every state must prepare for disruptive cyber events that affect public-facing services and critical internal operations.
Innovation	The response combined executive restoration priorities, a formal public-release decision gate, a single Recovery Hub, and state-led technical recovery rather than ransom payment.

IDEA

Cybersecurity readiness is often invisible until it is not. Nevada's opportunity was to prove that its incident response program, cross-agency governance, vendor readiness, and continuity planning could operate under real-world pressure without transferring public dollars to criminal actors.

The incident affected essential systems across state government, which meant the business problem was broader than technology restoration. Nevada needed to protect public safety, keep payroll on schedule, preserve benefits and fiscal operations, communicate lawfully without helping the attacker, and restore trust while hardening the environment.

- The response relied on a formal Incident Response Plan with immediate escalation to the CIO, Governor's Office, critical agencies, legal counsel, and law enforcement partners.
- The State used a risk-based prioritization model focused on life and safety, statutory and fiscal obligations, and continuity of citizen-facing services.
- Communications followed an "execute, then communicate" model: safety first, minimum necessary technical detail, coordinated public messaging, and lawful transparency.
- The project addressed universal state priorities: cybersecurity, risk management, data protection, continuity of operations, public trust, and responsible stewardship of taxpayer funds.

Why it matters: Nevadans do not experience cybersecurity as a firewall rule. They experience it as whether payroll runs, benefits systems work, records are available, emergency communications continue, and public agencies can serve them when things go wrong.

IMPLEMENTATION

GTO moved through four coordinated workstreams: containment and investigation, executive prioritization, secure restoration, and post-incident hardening. Affected systems were isolated, access was re-established through controlled channels, and forensic review determined scope and informed eradication. Recovery planning prioritized the most critical functions first, rather than treating every outage as equal.

The Governor's Office and State CIO established daily priorities and decision gates. Internal leadership received frequent situational updates, agency IT leads received operational guidance, and the public Recovery Hub served as the plain-language source of truth. Service restoration notices were issued only after validation and rollback paths were in place.

- Partner coordination: state agencies, critical vendors, law enforcement, privacy/legal counsel, and executive leadership worked from a shared operating picture.
- Recovery sequencing: payroll, public safety, eligibility systems, fiscal distributions, courts, DMV customer services, emergency management, and other high-impact functions were sequenced based on public need.
- Hardening: the State implemented account cleanup, password resets, privilege review, access-control remediation, segmented access, enhanced monitoring, and strengthened administrative controls.
- Future-state roadmap: GTO identified SOC maturity, endpoint detection and response, device hardening, patching, privileged access management, legacy protocol reduction, and employee training as ongoing investments.

Workstream	Operational value
Containment and investigation	Stopped further spread, preserved evidence, determined scope, and enabled targeted eradication.
Continuity and prioritization	Focused scarce recovery capacity on services with the greatest public impact.
Secure communications	Kept agencies and the public informed without publishing details that could increase attacker leverage.
Hardening and sustainment	Converted recovery lessons into identity, endpoint, monitoring, and training improvements.

IMPACT

Nevada's response turned a severe cyber event into a measurable resilience outcome. The State did not pay ransom, restored business-critical services within seven days, completed statewide full-service recovery in 28 days, recovered approximately 90% of impacted data, and maintained essential state operations through a state-led surge model.

The response also demonstrated fiscal stewardship. Fifty State employees logged 4,212 overtime hours at a direct overtime cost of $210,599.87 and a fully loaded estimate of $259,037.84. Compared with a conservative contractor-equivalent surge at $175 per hour, the State avoided an estimated $478,062 while retaining institutional knowledge and tighter change control.

Impact area	Measured result
Service restoration	Business-critical services restored within seven days; full-service recovery completed in 28 days.
Ransom posture	No ransom paid; public funds were directed to recovery, hardening, and expert support instead of criminal actors.
Data recovery	Approximately 90% of impacted data recovered and remaining data addressed through risk-based review.
State workforce surge	4,212 overtime hours from 50 employees; estimated fully loaded cost of $259,037.84.
Cost avoidance	Estimated $478,062 avoided compared with a $175/hour contractor-equivalent model.
Long-term maturity	Roadmap established for SOC, EDR, identity protection, OS hardening, patching, and security training.

Testimony

Voice from the field: The response validated years of strategic planning, incident simulations, legislative support, and vendor readiness. It also reinforced a hard lesson of public service technology: resilience is not what you buy after the incident. It is what you build before the incident, then prove under pressure.

What Now

- Retain the Recovery Hub and public-release decision gate as standing communication controls.
- Advance centralized security operations and endpoint detection across the enterprise.
- Expand identity protection, privileged access controls, OS hardening, patch compliance, and workforce training.
- Continue after-action exercises and vendor readiness reviews so lessons remain operational, not decorative.