State of Nevada – Governor's Technology Office

AFTER ACTION REPORT

2025 Statewide Cyber Incident

INFO~TECH RESEARCH GROUP

October 28th,2025

Table of Contents

Statement From the CIO

The State of Nevada's Governor's Technology Office (GTO), under the leadership of the Office of the CIO, coordinated the remediation of a targeted cybersecurity breach that disrupted state systems for approximately 28 days. The incident was initiated through a Search Engine Optimization poisoning campaign where an attacker embedded malicious code into a trusted online resource frequently accessed by state IT personnel. This code was downloaded and installed on an internal workstation, bypassing endpoint defenses and granting unauthorized access to critical systems. The threat actor (TA) deployed an attack aimed at taking state systems offline and left behind a note with instructions on how to recover the encrypted systems and data, in an attempt to extort the State.

Upon identifying the breach, GTO staff acted promptly. Following established protocols and coordination, they initiated procedures to isolate affected systems and prevent lateral movement. Their quick response, supported by state-funded technology and strategic planning, halted the TA's progression and reduced further disruption.

Throughout the 28-day recovery period, the GTO coordinated efforts across more than 60 state agencies, six critical vendors, and eight supporting vendors, including law enforcement partners from local, state, and federal agencies. On day one, GTO provided hourly communications, and daily decisions were made in collaboration with IT leaders throughout the state and leaders across the Executive Branch. The State of Nevada decided not to pay the ransom demanded by the threat actor. This stance was maintained throughout the incident, and the State ultimately restored statewide services and recovered approximately 90% of the impacted data. The remaining 10% of affected data, while still in the State's control, was not required to restore essential services and is being reviewed on a risk-basis. While current analysis indicates low likelihood of material impact, we are maintaining enhanced monitoring and will take appropriate notification or remediation actions if new information emerges.

GTO's effectiveness was due to leadership from the highest levels of the executive branch, along with years of strategic investment in cybersecurity infrastructure, training, executive-branch wide collaboration, and legislative support. Their ability to mobilize incident response teams, conduct forensic analysis, and restore

operational integrity demonstrated their preparedness. Key partners such as Microsoft's PG, Cisco, and DELL were instrumental in achieving early restoration milestones within initial operational windows.

This incident highlights the importance of proactive defense and the critical role of GTO personnel in safeguarding public assets. The foresight of Executive Branch Leadership and the State Legislature in funding key cybersecurity initiatives helped ensure a potential full-scale ransomware event was contained and remediated. The resilience shown throughout this event reflects Nevada's technical capabilities and the dedication of the teams responsible for protecting them.

Timothy D. Galluzi, MBA, CPM, GCPM
Executive Director & State Chief Information Officer
Office of Governor Joe Lombardo | Governor's Technology Office

Summary Detail

On August 24, 2025, at 01:50 AM PDT, the State of Nevada's Governor's Technology Office (GTO) identified a system outage that resulted in multiple virtual machines (VMs) going offline. Demonstrating their preparedness, the GTO team followed their established Incident Response Plan. This plan included immediate escalation of the incident to the CIO, who then coordinated with the Governor's Office, critical State of Nevada agencies, and key leadership to ensure a unified and strategic response. Initially locked out of the systems, the GTO team successfully regained access using backup credentials and discovered encrypted files alongside a ransom note. They isolated the affected VMs to prevent further spread of the ransomware. Legal counsel from BakerHostetler LLP was engaged and promptly brought in Mandiant, a leading cybersecurity firm under Google Cloud, to conduct a **privileged forensic investigation**. This proactive approach enabled that the scope and nature of the attack were quickly understood, enabling the state to take decisive action.

The investigation revealed that the threat actor had infiltrated the system as early as May 14, 2025, when a state employee unknowingly downloaded a malware-laced system administration tool from a spoofed website. This tool installed a hidden backdoor, which remained active despite Symantec Endpoint Protection quarantining the tool on June 26. The attacker escalated their access by installing a commercial remote monitoring software, on multiple systems, compromising both standard and privileged user accounts. By mid-August, the attacker had established encrypted tunnels and used Remote Desktop Protocol (RDP) to move laterally across critical systems, accessing sensitive directories and even the password vault server. On August 24, the attacker deleted backup volumes and deployed ransomware, encrypting VMs and disrupting critical services. Thanks to the GTO's rapid response and seamless collaboration with cybersecurity experts, the threat was containment measures were implemented quickly. Recovery protocols were initiated immediately, minimizing the impact and ensuring the continuity of essential state operations. This incident underscores the importance of having a well-rehearsed incident response plan and trusted partnerships with legal and cybersecurity professionals. The incident further highlighted the importance of robust cybersecurity measures and the value of preparedness, and the critical role of **staff training and awareness** in mitigating cyber risks.

Threat Actor Actions

Between August 16 and August 24, the threat actor accessed multiple critical servers, including the password vault server, and retrieved credentials from 26 accounts. They meticulously cleared event logs to obscure their activities. On the day of the ransomware deployment, the attacker deleted backup volumes and altered security settings to facilitate the execution of unauthorized code. At 01:30 AM PDT, ransomware was deployed, encrypting VMs and disrupting critical services. Despite these challenges, the State of Nevada's response was commendable. The GTO's ability to quickly isolate affected systems and engage expert assistance minimized the impact and laid the groundwork for recovery.

Investigation

The State of Nevada's strategic foresight in securing cyber insurance, a key initiative supported by the state legislature over the past three years, proved instrumental during the cyber incident on August 24, 2025. Upon detection of the ransomware attack, the state's cyber insurance provider recommended Mandiant, a globally recognized cybersecurity firm under Google Cloud, to lead the investigative response due to their deep expertise in handling sophisticated ransomware threats. This pre-established relationship enabled the state to act swiftly and decisively. Mandiant was formally engaged on August 26, 2025, and their analysis concluded on September 9, 2025. A final confidential and technical report was issued to GTO for review on October 10th, 2025.

Mandiant's primary objectives during the engagement were comprehensive and critical to the state's recovery.

First, they worked to determine the full scope of the intrusion and confirm whether the threat actor (TA) remained active within the environment. Their investigation found no evidence of ongoing activity at that time, allowing the State to focus on containment and recovery.

Second, Mandiant identified the earliest date of compromise as May 14, 2025, and traced the cause to a malware-laced system administration tool downloaded by a state employee.

Third, they assessed the type and extent of data exposed, identifying that 26,408 files were accessed and 3,241 files were exposed across multiple systems.

A zip file containing sensitive data, split into six parts, was also created by the TA. Of the files compressed and packaged for exfiltration, only one document was assessed to contain personal information as defined by NRS 603A.040. That file identifies a former state employee who was notified by the State pursuant to NRS 603A.220. While these files were packaged for transport, the investigation team found no confirmation to date of successful extraction or publication on a TA leak site; monitoring continues.

Additionally, Mandiant provided valuable intelligence on the TA's tactics, techniques, and procedures (TTPs), including the use of the backdoor, monitoring software, and encrypted tunnels for lateral movement. This intelligence was crucial in understanding the adversary's capabilities and intentions. Mandiant also collaborated with the Governor's Technology Office (GTO) to develop a tailored containment and eradication plan, executing eradication steps; no persistence was observed post-remediation, and enhanced monitoring continues.

The comprehensive documentation and supplemental reports provided by Mandiant enabled the state to accurately assess the potential exposure and communicate findings to stakeholders. This incident underscores the effectiveness of Nevada's cybersecurity protocols, the value of strategic planning, and the importance of continuous vigilance. The state's swift coordinated response not only mitigated the damage but also reinforced public trust in its digital infrastructure.

Evidence of Compromise

The earliest evidence of TA activity occurred on May 14, 2025, at 23:46:03 UTC (04:46 PM PDT). At that time, a State Employee downloaded and executed a malware-laced version of a system administration tool twice from a website posing as the legitimate hosting site. Further adding to the complexity of the deception, the TA leveraged legitimate Google advertisements as a vector to deliver the malware package. This action immediately configured a hidden backdoor that established a connection to the TA's infrastructure each time a user logged onto the system. Although Symantec Endpoint Protection (SEP) quarantined and then deleted the malicious system administration tool on June 26, 2025, the configured underlying persistence mechanism was not removed and continued to remain active.

On August 5, the TA installed a commercial remote monitoring software, on a user's system that allows for screen recording and logging user keystrokes. On August 15,

2025, the TA installed the remote monitoring software on another user's system. Analysis revealed that the TA compromised both the standard and privileged accounts for the primary users of the two systems on which remote monitoring software was installed.

The TA then shifted to escalating privileges and moving laterally, which began on August 14, 2025, when the TA deployed a customized, encrypted tunnel to bypass security controls and facilitate Remote Desktop Protocol (RDP) access in the environment.

Between August 16 and August 24, the TA used RDP to move between critical servers, accessing multiple directories, files, and servers—including the password vault server—to retrieve passwords from 26 accounts. The TA consistently cleared event logs to hide their activity.

On August 24, 2025, in preparation for the ransomware deployment and to prevent recovery, the TA authenticated to the backup server and deleted the backup volumes. The TA then logged into the VM centralized management server using the root account and changed security settings to allow unauthorized code to run. Finally, at 08:30:18 UTC (01:30 AM PDT), the TA deployed the ransomware onto the virtualization servers hosting VMs, which encrypted VMs and resulted in critical services being taken offline.

Timeline

Date	Event	Phase
2025-05-14	Initial compromise via social engineering	Compromise
2025-06-26	Endpoint Protection quarantined Malicious tool, backdoor persists	Compromise
2025-08-15	Attacker escalates access and installs monitoring software	Escalation
2025-08-24 01:52	Outage detected, VMs offline	Response
2025-08-24 07:37	Incident escalated to CIO and Governor's Office	Response
2025-08-24 09:51	Access regained, encrypted files and ransom note found	Response
2025-08-24 12:37	Affected VMs isolated to prevent spread	Response
2025-08-24 16:44	Legal counsel and Mandiant engaged	Response
2025-08-24 ≈17:03	Recovery protocols initiated	Recovery

Initial Indicator of Compromise (IOC)

The State of Nevada – Governors Technology Office encountered a highly targeted cybersecurity breach initiated through a social engineering campaign. The threat embedded itself within a trusted online resource frequently accessed by IT administrative personnel. The malicious code was downloaded and installed on an internal workstation, bypassing endpoint defenses and granting unauthorized access to critical systems. This allowed the threat actor (TA) to deploy a coordinated attack to disrupt system functionality. The TA left behind a file containing instructions to recover state systems and data.

Upon identification of the attack, GTO staff acted promptly. Leveraging established protocols and cross-functional coordination, the team-initiated containment procedures to isolate affected systems and prevent further spread of the threat. The rapid response was instrumental in halting the TA's progression and minimizing additional disruption.

Despite the initial impact, which included system outages and recovery costs, the GTO's preparedness and execution enabled the State to mitigate more severe consequences. The team's ability to mobilize incident response teams and vendor resources, conduct forensic analysis, and restore operational integrity was a direct result of prior investments in cybersecurity infrastructure, training, and strategic planning.

Investigation

The alerting system provided real-time notifications, prompting immediate investigation. Within minutes, the issue was escalated to on-call staff. Over the next few hours, it was confirmed to be a ransomware event. GTO followed its escalation protocols, engaging critical vendors, some of whom flew on the same day to assist. During the investigation, it was discovered that backup data had been deleted, extending the recovery timeline. Nevertheless, GTO activated pre-planned incident response playbooks and mobilized support from Microsoft's Disaster and Recovery Team (DART), and other vital partners such as Broadcom, DHS, and the FBI. Thanks to years of building strong vendor relationships, which enabled rapid forensic analysis and recovery. Despite the loss of data backups, DELL being a critical partner of technology was able to successfully restore the majority of data within 28 days, with residual items tracked through standard remediation. The recovery

process was based upon the critical nature of the agencies and services provided to our citizens in attempt to reduce the impact on our citizens.

Response Detail

GTO's primary focus initially was on isolation before GTO could look at how best to start system and data recovery. Upon discovering the loss of backup data, GTO engaged DELL Recovery Support, which successfully recovered approximately 90% of our data over a 28-day period. Recovery efforts prioritized critical systems first, followed by less essential ones. Daily communications with field agencies, adherence to incident response playbooks, and a dedicated recovery team were key contributors. The success of this operation is rooted in the last five years of strategic incident response planning by GTO, supported by legislative funding for cyber insurance, fault-tolerant vendors, and specialized staff. Vendors played a vital role: Mandiant provided intrusion analysis, DELL led data recovery, and Microsoft supported O365 restoration. Continuous vendor support and prior funding were instrumental in validating remediation efforts.

This incident underscores the importance of proactive defense and the critical role of GTO personnel in safeguarding public assets. Thanks to their efforts and the foresight of the State Legislature in funding key cybersecurity initiatives, what could have escalated into a full-scale ransomware event was effectively contained and remediated. The resiliency demonstrated throughout this event reflects both the strength of our technical capabilities and the dedication of the teams entrusted with protecting them.

This incident reaffirmed the importance of continuous maturity in incident response and continuity of operations planning across the state government. Ongoing testing and training of state staff remain critical factors for continued maturity. Annual evaluations of vendor support services are essential. Moving forward, GTO have identified the need to move away from our current de-centralized security services model. GTO will be reviewing options for the implementation of a hybrid security services model that has a centralized Security Operation Center (SOC) monitoring of critical infrastructure with the addition of a unified Endpoint Detection and Response (EDR) system. At the agency level, GTO discovered that application ownership is an issue and requires additional process improvements and regular review. The use of non-technical teams like the GTO Project Management Office

(PMO) and reinforcing sensitive communication protocols with external PR support are important components. GTO's IT and security vendor program has provided valuable insights into additional security for system and data backups.

Leadership and Support

This coordinated response was the result of years of strategic planning and regular preparedness exercises. The State of Nevada had invested in annual cybersecurity incident response simulations, which proved invaluable in this real-world scenario. These exercises, conducted across multiple agencies and leadership levels, ensured that all stakeholders were familiar with their roles and responsibilities during a cyber crisis. As a result, when the incident occurred, the Governor of Nevada, the Governor's Office, the Governor's Technology Office (GTO), the Chief Information Officer (CIO), the Attorney General's Office, Risk Management, and agency leadership were able to act swiftly and cohesively. The State Legislature's ongoing support for cybersecurity initiatives, including funding for training and simulation programs, further strengthened the state's readiness. These efforts enabled the seamless mobilization of resources and rapid decision-making, minimizing disruption to public services. The ability to execute a well-rehearsed response plan under pressure demonstrated the maturity of Nevada's cybersecurity posture. It also highlighted the value of cross-agency collaboration and executive-level engagement in managing high-impact incidents. This level of preparedness not only protected critical infrastructure and sensitive data but also reinforced public confidence in the state's ability to respond to evolving cyber threats.

Communications and Coordination

When a cyber incident hits, words can help—or they can give attackers a roadmap. Nevada chose a simple rule to balance transparency with public safety: execute, then communicate. GTO prioritized actions that made Nevadans safer (containment, credential resets, access hardening, service restoration), then explained those actions promptly, clearly and without details that could aid the attacker.

What "execute, then communicate" meant in practice: it meant safety first, minimum necessary technical detail, coordinated voice and lawful transparency. GTO contained systems, rebuilt trust, rotated credentials/keys, and restored essential services before sharing operational specifics. GTO described what

Nevadans needed to know (status, impacts, what to do) without sharing how controls were configured or exactly when cutovers would occur. Spokespersons and message owners were pre-assigned; the state CIO for technical posture and milestones; Governor's Office for statewide framing and public reassurances; OEM/DEM PIOs for public information alignment; and agency PIOs for program-specific notices. GTO were open about service status and recovery while protecting investigative integrity and security posture, consistent with NRS 242.105 and NRS 241.020(4)(b).

Cadence and Channels

On Day zero, internal leadership received hourly situational updates and the public was notified of intermittent availability. During Days 1–7, the rhythm included a morning operational brief, a midday status sync, and an end-of-day roll-up with next-day priorities. Weeks 2–4 emphasized scheduled progress updates tied to verified milestones. The public **Recovery Hub** (oem.nv.gov/recovery) served as the single source of truth for plain-language status, "what to expect," and help contacts; agency pages pointed back to the hub to avoid version drift. ISO/IT lead bulletins covered identity-verification windows, password/MFA steps, the prohibition on hosts-file workarounds, VPN re-enablement sequencing, and issue routing. A PIO working group produced daily "three bullets" (unavailable/limited services, modified hours/workarounds, what's next). Media handling emphasized consistent terminology, avoidance of real-time operational specifics, named points of contact for rapid fact-checking, and requests for editorial restraint where live details could elevate public-safety risk.

Decision Gate for Public Release

Before publishing, the State applied a four-question gate:

1. Will the disclosure help the public take the right action?
2. Could the detail increase attacker leverage or targetability?
3. Are law-enforcement or partner agencies requesting that specifics be held?
4. Has protective control already been executed (e.g., password resets, ACL changes)?

Where risk outweighed benefit, communications were summarized at a higher level and shared specifics only with need-to-know audiences. Notably, after early

briefings, firewall blocks and phishing attempts increased; sequencing communications **after** controls were live reduced attacker advantage while keeping Nevadans informed.

Public Meetings and Public Records

When the statewide posting site was intermittently unavailable, agencies proceeded under **NRS 241.020(4)(b)** by maintaining physical postings at customary locations, posting on agency sites, and consulting DAGs; centralized temporary reposting was avoided to limit single-point-of-failure risk. Public records requests were acknowledged and, where appropriate, narrowed; security-sensitive information was protected under **NRS 242.105** and the active-investigation doctrine; requesters were referred to correct custodians as needed. The State committed to releasing All-Agencies memoranda when appropriate. Federal and commercial partners received concise attestations covering segmentation, credential/key rotation, enhanced monitoring, and staged reconnection plans, with third-party letters provided when available and State memoranda used where external letters were pending.

Operational Alignment

Identity-hardening windows (07:00–19:00) were communicated only after verification stations were staffed and live. Service-restoration notices were issued after validation and rollback plans were in place. Media availability was aligned to concrete milestones (e.g., civil fingerprint system restored; FFL portal and phone lines live), ensuring the public received meaningful, time-relevant updates.

Sustainment

The State will retain the Recovery Hub as the canonical status source and expand plain-language FAQs and simple status indicators; maintain the execute-then-communicate gate as a standing control; continue the PIO “three bullets” and ISO channel discipline; and keep pre-staged NPRA templates (acknowledgment, narrowing, exemption, refer-to-custodian) and an Open Meeting Law technical-issues note ready for immediate use. This model preserves safety, supports lawful transparency, and ties communications directly to verified operational outcomes.

Executive Prioritization

The Governor's Office set and reaffirmed daily restoration priorities—centering life and safety, statutory and fiscal obligations, and public-facing continuity—and aligned both operational sequencing and public messaging to those priorities. Consistent with the **execution, then communicate** posture, milestones were announced only after controls were in place and validation was complete. The priority set included: Restoration of infrastructure for Payroll/Advantage 2.0/Core.NV; restoration of the front-facing portion of the Office of Emergency Management's website for dedicated messaging on status of recovery efforts; restoration of infrastructure for determining eligibility and access to the following programs (Division of Social Services): TANF/SNAP/Medicaid/Energy Assistance/Victims of Crimes; restoration of infrastructure to pay CTAX distributions from Taxation and PCFP distributions from NDE; restoration of the Dispatch/Records/NTAC systems of DPS (impacts LVMPD's fingerprinting and records system as well); restoration of the online systems for the Administrative Office of the Courts; restoration of NEBS/NEATS/CETS (for GFO budget close/IFC preparation); restoration of DMV customer-facing systems; NVHA infrastructure (district offices without remote access); OSIT's website public comment posting for BEAD; Department of Human Services facility automatic locks; DHS Electronic Health Records; Veterans Homes Electronic Medical Charting; restoration of VOIP to reinstate the Mobile Crisis Hotline (DHS); infrastructure for the Attorney General's Office (legal tracking/VPN); and Veterans Support Officers' access to the federal database.

Payroll Continuity

The Governor's Office designated payroll as a top restoration priority. Under tight timelines, the Governor's Technology Office isolated payroll processing from other recovery work, in support of executive-branch partners from the Office of Project Management, and Division of Human Resource Management, executed additional pre-run checks, and completed a post-run reconciliation before communicating outcomes. This **execute, then communicate** approach ensured employees and retirees were paid on schedule, avoided downstream disruptions to household finances, and maintained confidence in core state operations during the incident.

Operational Surge and Overtime (OT)

During the 28-day response and recovery, State technology teams sustained an emergency operational tempo to keep essential services moving. Between August 24 and September 20, a total of 4,212 overtime hours were logged by 50 State employees across GTO and partner divisions, at a direct overtime wage cost of $210,599.87 (fully loaded estimate: $259,037.84). That surge capacity—nights, weekends, and holidays—meant payroll processed on time, public safety communications stayed online, citizen-facing systems returned in phased order, and agencies received daily guidance while core platforms were rebuilt.

What this Bought Nevada

- **Continuity of pay and mission-critical operations.** Overtime staffing preserved payroll runs and kept high-impact functions (dispatch/records, eligibility systems, court portals, DMV customer systems) on a path to restoration despite the loss of backups and the scale of reconstitution required.
- **Speed to recovery**. The State reached full-service recovery in 28 days—well below typical public-sector timelines for incidents of this scope—because in-house staff could execute 24×7 playbooks alongside vendors and law enforcement.
- **Fiscal responsibility.** Leveraging State teams for surge work contained costs compared to an all-contractor model.

Cost comparison **(conservative scenarios)**

Item	Value
State OT hours	4,212
State OT direct cost	$210,599.87
Fully loaded estimate (benefits/shift diff)	$259,037.84
Contractor-equivalent @ $150/hr	$631,800.00
Contractor-equivalent @ $175/hr	$737,100.00
Contractor-equivalent @ $200/hr	$842,400.00
Estimated savings vs. $175/hr	$478,062.16

How to read this: even using a conservative fully loaded OT figure, the State avoided significant outside-labor cost—while retaining institutional knowledge, tighter change control, and faster hand-offs with agency partners. This is a clear example of fiscal discipline and operational maturity under stress.

Scope of Impact

The ransomware attack on August 24, 2025, impacted over 60 state government agencies, disrupting essential services across county and local governments. Among the most critical agencies affected were the Department of Health and Human Services, the Department of Motor Vehicles, and the Department of Public Safety. These agencies provide vital services to Nevada's citizens, including healthcare access, public safety, and transportation. The State's ability to respond effectively was rooted in years of strategic planning, including the cultivation of strong vendor relationships. These partnerships—established through prior initiative proved invaluable during the crisis, enabling rapid mobilization of expert resources and tools. The collaborative response between state leadership and trusted vendors ensured that the incident was isolated, investigated, and ultimately resolved with minimal long-term disruption.

Day 0 (August 24, 2025): The Governor's Technology Office (GTO) identified a significant system outage and immediately escalated the issue to the Governor's Office. Upon investigation, a ransom note was discovered, confirming a ransomware attack. The GTO team acted swiftly to isolate the affected virtual machines (VMs), preventing further spread of the malware. This early containment was critical in preserving unaffected systems and maintaining operational integrity across other state services.

Executive Priorities and Restoration Sequencing

The Governor and his office began work to identify all impacted systems in conjunction with cabinet level officials and other executive branch leadership on day 0, shortly after the incident started. They began formulating the priority list for restoration with the State CIO. As soon as the list was compiled, the Governor's Technology Office was provided clear, actionable priorities that governed restoration sequencing, resource allocation and communications. These directives emphasized protection of life and safety, fulfillment of statutory and fiscal obligations, and continuity of

essential public services. The Governor's Technology Office operationalized these priorities through daily tasking, identity-verification windows, and controlled service re-enablement; communications mirrored this sequence, announcing milestones only after validation and rollback paths were safely in place. The prioritization of restoration list was intended to provide an adaptive method for resources allocation to address high priority needs as issues developed and challenges were identified.

Application. Office of Project Management (OPM) and Office of Information Security (OISCD) translated these priorities into daily schedules and work queues, allocating verification slots, identity hardening, ACL changes, and phased re-enablement accordingly. The public Recovery Hub highlighted progress against these priorities in plain language; media availabilities and agency bulletins followed the same order, reinforcing clarity and consistency for stakeholders.

- ✓ **Day 1:** The State activated its vendor response teams, including Mandiant, Microsoft DART, Broadcom, and Dell. These partners were selected based on pre-established relationships and their proven expertise in cybersecurity and infrastructure recovery. Their rapid deployment allowed for immediate forensic analysis, containment planning, and system triage. Public communication was also issued to inform citizens and stakeholders of the incident, reinforcing transparency and trust. This was the first 'Business Day' of the cyber event. The Governor's Office made the difficult call, understanding the impact to constituents, to close state offices to allow IT Teams time to ensure that the TA activities were isolated, and recovery efforts could begin safely.
- ✓ **Day 2 A.M.:** A second round of public communication was released, providing additional details about the nature of the cyber incident and the steps being taken to address it. This update helped manage public expectations and reassured citizens that recovery efforts were underway. The communication emphasized the collaborative efforts between state agencies and private sector partners.
- ✓ **Day 4:** A comprehensive recovery plan was finalized and communicated to all stakeholders. This plan outlined the phased restoration of services, prioritizing critical systems that directly impacted public welfare. The plan

also included enhanced monitoring and security measures to prevent further compromise.

- ✓ **Day 5:** The recovery timeline was shared with internal and external stakeholders, including agency leadership, legislative partners, and the public. This timeline provided clarity on service restoration expectations and demonstrated the state's commitment to accountability and transparency.
- ✓ **Day 15:** The Governor's Office issued ongoing updates, highlighting progress made and reaffirming the state's dedication to full recovery. These updates maintained public confidence and highlighted the effectiveness of the coordinated response.
- ✓ **Day 28:** Restoration of services was completed statewide. Systems were restored, data integrity checks were completed and issues addressed, and enhanced security protocols were implemented. The successful resolution of the incident underscored the strength of Nevada's cybersecurity strategy, the value of interagency coordination, and the critical role of trusted vendor partnerships.

Ransom Payment

The State of Nevada maintains a firm position against paying any ransom demands from threat actors, a stance rooted in its comprehensive and continually evolving Incident Response (IR) program. Over the past several years, the State has strategically invested in strengthening its cybersecurity posture through increased funding, the adoption of advanced technologies, and the recruitment of skilled cybersecurity professionals. These enhancements have been guided by a commitment to resilience, ensuring that the State can respond effectively to even the most sophisticated cyber threats. The IR program emphasizes preparation, containment, recovery, and communication, all of which were executed with precision during the August 2025 ransomware incident. The decision not to pay a ransom was not made lightly; it was the result of confidence in the State's ability to recover through its own capabilities and trusted vendor partnerships. By leveraging robust backup and recovery systems, the State was able to restore critical services without compromising its principles or encouraging future attacks. Key vendors, including Mandiant, Microsoft DART, Broadcom, and Dell, played an essential role in supporting the recovery process, validating the importance of long-standing vendor relationships as a core component of the State's cybersecurity strategy. The

coordinated efforts between internal teams and external partners ensured that data integrity was preserved and services were restored efficiently. This approach demonstrated fiscal responsibility by avoiding the financial and ethical pitfalls of ransom payments. It also reinforced the State's commitment to protecting taxpayer resources.

Financial Response: Strategic Investment in Resilience

The State of Nevada's decision not to pay the ransom was a strategic choice enabled by prior investments in cyber insurance and robust vendor partnerships. While this stance prevented state funds from going to criminal actors, the recovery required a significant and immediate financial commitment to engage elite cybersecurity and technology expertise. The total obligated cost for external vendor support during incident response was **$1,314,200**. These were not unforeseen expenses; they were activations of pre-negotiated contracts designed for exactly this scenario. Engaging critical vendors within hours was essential to contain the threat and begin secure recovery without delay.

What these funds delivered

Forensic investigation and threat intelligence (Mandiant): Scope confirmation, adversary TTPs, and assurance of full eradication.

Infrastructure recovery and hardening (Microsoft DART, Dell): Secure rebuild of critical systems (including Active Directory), restoration from viable sources after backups were destroyed.

Specialized recovery and engineering support (Aeris): Agile, on-the-ground assistance that accelerated tempo during key windows (including a successful payroll cycle).

Legal and privacy counsel (BakerHostetler): Guidance on notification, compliance, and investigative coordination.

Obligated vendor costs to date (summary)

Vendor	Service Provided	Obligated Cost
Microsoft DART	Unified Support & Infrastructure Rebuild	$354,481
Mandiant	Forensics & Incident Response	$248,750
Aeris	Recovery & Engineering Support	$240,000
BakerHostetler	Legal & Privacy Counsel	$95,000
SHI (Palo Alto)	Network Security Services	$69,400
Dell	Data Recovery & Project Management	$66,500
Other IR Vendors	Various Support Services	~$240,069

Why this was fiscally responsible

Investing in resilience and recovery capabilities is more effective—and more accountable—than paying ransom. These dollars went to trusted, expert partners who resolved the immediate crisis **and** left the State with a hardened, more defensible environment. The result: faster restoration, preserved public trust, and enduring value for Nevadans.

Recovery Actions

Under the direction of trusted vendors, the Governor's Technology Office (GTO) implemented a series of critical hardening measures to strengthen the state's cybersecurity defenses. These actions were part of a coordinated response effort, reflecting strategic partnerships and technical readiness. The GTO focused on securing the most sensitive systems first, ensuring that access was limited to essential personnel. They cleaned up old or unnecessary accounts, reset passwords, and removed outdated security certificates. The team also reviewed and reinforced system rules and permissions to prevent unauthorized access. Shared folders and login scripts were scanned for threats, and new security tools were deployed to monitor and enforce protection policies. These efforts were both technical and strategic, aimed at enhancing the State's overall cyber defense posture.

The collaboration between internal teams and external partners gave state leadership the confidence that the situation was under control and that long-term improvements were being made to prevent future incidents.

The changes included:

- ✓ The team organized computer systems into different levels based on how important they are. It's like putting your most valuable things in a locked box and less important things in a regular drawer. This helps protect the most important systems better.
- ✓ They made special new accounts for the most important systems and made sure no one else could use them. It's like giving a key to a secret room only to the most trusted people and making sure no one else can copy it.
- ✓ The team connected special rules to each level of the system to control what people can and can't do. It's like setting up rules for each room in a house – some rooms are off-limits unless you have permission.
- ✓ Team checked who had special powers in the system and removed anyone who didn't need them. It's like making sure only the right people have the keys to important places.
- ✓ They cleaned up who had access to the most important parts of the system. Think of it like checking who has the master keys to the whole building and taking them away from people who shouldn't have them.
- ✓ GTO looked over the rules for the most important systems to make sure they were safe and correct. It's like double-checking the locks on the most valuable rooms in a building.
- ✓ Investigators searched for shared folders to make sure no bad files were hiding there. It's like checking your backpack to make sure no one slipped something in without you knowing.
- ✓ They used special tools to make sure the most important systems followed the right rules. It's like using a remote control to lock all the doors in a building at once.
- ✓ GTO had to change passwords to make sure the bad guys couldn't get back in. It's like changing all the locks in your house after someone tried to break in.
- ✓ GTO replaced a special digital key that helps keep secrets safe. It's like getting a brand-new master key that only trusted people can use.

- ✓ They got rid of old or unused security certificates that could be misused. It's like throwing away expired ID cards so no one can use them to sneak in.

Recommendations

The Governor's Technology Office (GTO) implemented a series of recommendations for hardening measures to strengthen the state's cybersecurity defenses. These actions were part of a broader strategy that had been developed and refined over the 28-day recovery period, supported by vendors, advanced technologies, and the GTO personnel. The GTO focused on securing the most critical systems first, ensuring that only authorized individuals had access to sensitive areas. They removed outdated or unnecessary user accounts, reset passwords across all systems, and replaced old digital keys to prevent unauthorized access. The team also reviewed and updated system rules and permissions, ensuring that only the right people could make changes to important settings. Shared folders and login scripts were scanned for hidden threats, and new security tools were deployed to monitor and enforce protection policies. These efforts were not only technical but also strategic, reflecting a mature and proactive approach to cyber defense.

The collaboration between internal teams and external partners gave state leadership confidence that the situation was under control and the following recommendations addressed:

1. **Preventing Hackers from Moving Around (Lateral Movement Risk)**
   To stop hackers from moving freely inside systems once they get in, the state began adopting additional zero-trust methodologies, GTO implemented enhanced segmentation between agencies based on operational needs. GTO strengthened Access Control Lists (ACLs) to restrict access between administrator-level domains and tightened firewall rules to reduce and block unfiltered or unnecessary applications and services. Additionally, GTO made sure that regular user accounts and powerful admin accounts are kept separate. This is like having different keys for your bedroom and a bank vault—just because someone can enter the house, it doesn't mean they can open the safe. By organizing access this way, GTO make it much harder for attackers to reach the most important systems if they break in somewhere else.

2. **Protecting Powerful Accounts (Privileged Access Risk)**
   GTO made sure that special accounts with lots of power can't be used by others or passed around. This is like putting a "do not share" label on a master key so no one else can borrow it. It helps prevent hackers from stealing these keys and using them to take over important systems.
3. **Keeping Passwords Safe (Credential Access Risk)**
   GTO checked for accounts that could be tricked into giving away their passwords and made changes to stop that from happening. This included removing extra permissions, using safer types of accounts, and cleaning up anything that wasn't needed. These steps help stop hackers from stealing passwords and using them to sneak into Nevada's systems.
4. **Stopping Sneaky Power Grabs (Privilege Escalation)**
   GTO found some accounts that had too much control and could change important settings, even though they weren't supposed to. GTO fixed this by taking away those powers from the wrong accounts. This makes sure only the right people can make big changes, keeping the State's systems safer.
5. **Giving Only the Right Amount of Access (Principle of Least Privilege)**
   GTO noticed that some people had more access than they needed, especially in very sensitive areas. GTO took away those extra permissions and double-checked the rules that decide who can do what. This helps reduce the chances of mistakes or misuse, and it keeps the most important systems locked down tight.

Recovery Success

The State of Nevada's full recovery from the ransomware incident was just 28 days. This stands out as a significant achievement, especially when compared to the national average recovery time for similar events, which often extends well beyond a month. This accelerated timeline was not coincidental, it was the result of years of strategic planning, investment, and maturity in cybersecurity readiness. The Governor's Technology Office (GTO), in close coordination with critical vendors, and federal partners, led a well-orchestrated response that prioritized speed, precision, and resilience. At the heart of this success were thoroughly prepared and regularly tested incident response playbooks, which provided clear guidance during a time of crisis. Business-critical services were restored within the first seven days, ensuring that essential functions for citizens continued with minimal disruption. The recovery

effort included a full rebuilding of the Active Directory, deployment of a Tiering Model to better protect accounts, cleanup of access control lists (ACLs), and implementation of Windows Local Administrator Password Solution (LAPS) to enhance password security. These technical milestones were executed with precision and timeliness by both vendor and state teams. While the response was a team effort, it was clearly led by the State and the GTO, demonstrating strong leadership and ownership throughout the process. The ability to recover quickly and securely was a direct reflection of the maturity of Nevada's cybersecurity program. Years of investment in people, processes, and partnerships paid off when it mattered most. This event validated the importance of proactive planning and reinforced the value of maintaining strong relationships with trusted vendors and partner agencies. It also showcased the effectiveness of a unified response model where public and private sector teams work seamlessly together. The 28-day recovery not only minimized operational downtime but also strengthened public trust in the state's digital resilience. Nevada's experience serves as a model for how strategic foresight and disciplined execution can dramatically reduce the impact of even the most serious cyber threats.

Coordination and Praise

The response to the ransomware incident showcased not only the State of Nevada's preparedness but also the exceptional capability and professionalism of the Governor's Technology Office (GTO) staff. From the outset, the response was a coordinated effort involving the Governor's Office, over 60 state agencies, five critical support vendors, and federal law enforcement partners including the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). Despite the complexity of the incident, the State led the response with clarity and confidence, setting the tone for a unified and effective operation. The GTO staff demonstrated deep technical expertise, calm under pressure, and a clear understanding of their roles, which earned high praise from multiple vendor partners. Microsoft's DART team specifically commended the State's rapid response and overall readiness, noting that Nevada's approach was among the most organized they had encountered. Dell highlighted the seamless collaboration and the efficiency of the recovery efforts, emphasizing how well the State and vendor teams worked together. The State extends sincere thanks to **Aeris**, a small Reno-based team whose around-the-clock support materially improved the tempo and

reliability during recovery, directly supporting the state's payroll needs. Aeris helped coordinate operational communications, provided hands-on engineering assistance during critical windows (including the successful payroll cycle), and consistently modeled calm, solutions-focused professionalism. Their local presence and agility amplified GTO's efforts and delivered real value to Nevadans when it mattered most. These endorsements reflect the success of years of investment in training, process development, and relationship-building with trusted partners. The State's ability to lead the response while leveraging vendor expertise exemplified a mature and proactive cybersecurity posture. The GTO's leadership ensured that all actions were executed with precision and timeliness, contributing to the rapid restoration of services. This level of performance not only accelerated recovery but also reinforced the State's reputation as a national leader in public sector cybersecurity. The incident response demonstrated that Nevada's approach to cybersecurity is not only strategic but also operationally effective. The collaboration between internal teams and external experts was a model of public-private partnership in action. Ultimately, the State's readiness and the professionalism of its teams turned a potentially devastating event into a story of resilience and success.

Future Cybersecurity Needs

While the State's response to the ransomware incident was a clear success, it also highlighted the importance of continued investment in cybersecurity. To maintain and strengthen Nevada's ability to respond to future threats, GTO must expand their monitoring and response capabilities. As cyber threats grow more sophisticated, so too must the tools, processes, and staffing. The incident demonstrated that GTO's current strategies are effective, but to stay ahead, GTO must evolve. This includes enhancing real-time threat detection, increasing automation in response workflows, and expanding visibility across all systems. Continued collaboration with trusted vendors will be essential in this journey, ensuring GTO has access to the latest technologies and expertise. Additionally, GTO must invest in training and retaining skilled personnel who can operate and adapt these tools effectively. These future-focused efforts will support our ongoing cybersecurity maturity and ensure the continuity of operations for all state agencies and the citizens they serve.

The following are strategic projects and initiatives to support our journey:

Security Operations Center (SOC)

To continue strengthening Nevada's cybersecurity posture, GTO must invest in the maturity of its people, processes, and technology. Recommendations include prioritizing continuity of operations are essential, especially in preparing for emerging threats like AI-generated attacks. The State of Nevada - Governors Technology Office is now implementing recommended security protocols, pursuing a centrally managed SOC, and improving third-party site processes and backup recovery. These efforts require funding to support hybrid security services, monitoring, alerting, and training across all state agencies. GTO will be prepared to justify these investments and value they provide to the citizens of Nevada. GTO thanks the State Legislature for its continued support and look forward to building a proactive secure and resilient program.

GTO is implementing a centralized SOC to monitor real-time traffic across all state, local, and municipal agencies. This initiative will provide enhanced visibility into network activity, enabling faster detection and response to threats. The SOC will unify monitoring efforts, reduce response times, and support proactive defense strategies. It will also facilitate better coordination across agencies and vendors, ensuring a consistent security posture statewide.

Endpoint Detection and Response (EDR)

GTO is deploying a modern EDR platform to improve threat detection and response. This platform will offer advanced analytics, behavioral monitoring, and automated containment capabilities. It will enhance visibility into endpoint activity, reduce dwell time for threats, and support continuous improvement of detection capabilities. The EDR system will integrate with the SOC for centralized oversight.

Devices, Patching, and OS Hardening

GTO is implementing the Securing Privileged Access model to maintain control of Tier 0 assets. Service accounts are being restricted from interactive logins, with MSA or GMSA used for enhanced security. Domain controllers are being standardized to reduce the attack surface. A comprehensive patching strategy is being adopted for Microsoft and third-party products. Operating System hardening measures such as Credential Guard, Windows Hello for Business, SmartScreen, Application Control, Controlled Folder Access, Attack Surface Reduction, BitLocker, and Secure Boot are being enforced.

Identity Protection

GTO is enforcing Just-In-Time access for administration using PIM and PAM solutions. Strong authentication methods such as passwordless login, Hello for Business, FIDO, Microsoft Entra MFA, and OAuth tokens are being deployed. Legacy protocols like SMBv1, NTLM, TLS 1.0 and 1.1 are being inventoried and disabled. Services using outdated protocols like SMTP, Telnet, FTP, and IMAP are being updated to secure alternatives. These changes are essential for disabling legacy authentication and enabling Conditional Access.

Employee Training and Culture

GTO is expanding employee training programs to address future threats. Resources include the Microsoft 365 Security Center Learning Hub, Microsoft Learn, Ignite sessions, and the Microsoft Tech Community. Training focuses on threat recognition, secure practices, and incident response. Cultivating a strong security culture ensures that technological defenses and human behavior evolve together to mitigate risks.

Conclusion

The August 2025 ransomware incident served as a real-world test of the State of Nevada's cybersecurity readiness, and the results demonstrated the strength of years of strategic planning and investment. From the moment the threat was discovered, the Governor's Technology Office (GTO), in coordination with the Governor's Office and over 60 state agencies, led a swift and structured response. The incident response playbooks, which had been developed and tested over time, provided a clear roadmap for containment and recovery. Within hours, affected systems were isolated, and vendor partners were activated to support investigation and remediation efforts. The collaboration between state teams and critical vendors—including Microsoft DART, Dell, and others—was seamless and effective. Law enforcement partners such as DHS and the FBI were also engaged early, ensuring a comprehensive and secure response. The GTO's leadership and the professionalism of its staff were widely praised by vendors, who noted the State's exceptional preparedness and execution under pressure.

Following containment, the State transitioned into a recovery phase that prioritized both short-term restoration and long-term resilience. Business-critical services were restored within seven days, and full-service recovery was achieved in just 28

days—well below the national average, faster than many publicly reported public-sector timelines for incidents of similar scope. This success was made possible by the deployment of advanced technical solutions, including a full Active Directory forest rebuild, Tiering Model implementation, ACL cleanup, and Windows LAPS deployment. These efforts were executed with precision by the MOSSORBIT team and vendor partners, under the direction of the GTO. The incident also served as a catalyst for further hardening of the State's digital infrastructure, including mass password resets, privileged account reviews, and the removal of outdated security configurations. The State's refusal to pay ransom, backed by confidence in its recovery capabilities, demonstrated fiscal responsibility and a commitment to long-term cybersecurity maturity. This experience validated the effectiveness of Nevada's cybersecurity strategy and reinforced the importance of proactive planning and investment.

Looking ahead, the State recognizes that cybersecurity is a continuous journey, not a one-time achievement. While the response to this incident was a success, it also revealed opportunities to further enhance monitoring, detection, and response capabilities. The GTO is committed to expanding centralized monitoring, improving automation, and investing in workforce development to stay ahead of evolving threats. Continued support from the State Legislature will be essential to fund these initiatives and ensure the resilience of Nevada's digital government. Strengthening vendor partnerships, refining incident response playbooks, and conducting regular exercises will remain top priorities. These efforts will help ensure that the State can respond even more effectively to future incidents, minimizing disruption and protecting the services that Nevadans rely on every day. The August 2025 incident was a defining moment that showcased the State's ability to lead, adapt, and recover. It also laid the groundwork for the next phase of cybersecurity maturity, one built on collaboration, innovation, and resilience.

Authored By:

Mark A. Hellbusch
Director, Cybersecurity & Privacy Services
Info-Tech Research Group
www.infotech.com

Contributors:

Tim Galluzi
Executive Director & State Chief Information Officer

Michael Hanna-Brutos Meyering
Chief Communications & Policy Officer

Darla Dodge
Sr. Deputy, Chief Information Officer