



MIRASYS



CASE STUDY

Hyper-
Converged
Infrastructure

CASE STUDY BY MIRASYS, INC. COPYRIGHT 2026 MIRASYSUSA.COM



Introduction



For many technology operators, the ultimate goal is to **keep all systems online 100% of the time**. With natural disasters and other black swan events, this is a tall task, however, with solutions like Hyper-Converged Infrastructure this goal is more attainable than ever before.

Hyper-Converged Infrastructure (HCI) represents a fundamental shift in how critical systems are designed, replacing fragmented, hardware-dependent architectures with a unified, software-defined platform that integrates compute, storage, and networking into a single, resilient environment. By **eliminating single points of failure** and enabling features like automatic failover, node isolation, and rapid recovery, HCI is purpose-built for environments where uptime is non-negotiable. This case study demonstrates why that matters—showing how a real-world casino deployment leveraged HCI to withstand a catastrophic infrastructure failure that would have otherwise resulted in a *complete surveillance outage, regulatory shutdown, and millions in losses*. It is not a theoretical advantage; it is a proven safeguard when everything goes wrong.

01 | Research Proposal





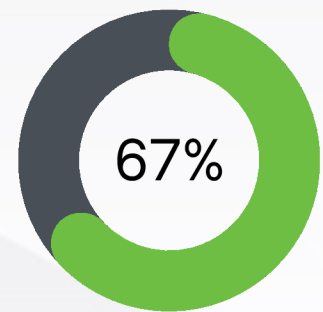
Problem Statement

In highly regulated casino environments, surveillance system uptime is not optional—it is mission-critical. A complete loss of video monitoring doesn't result in a delay or inconvenience; it triggers **an immediate, mandatory shutdown**. For operations running 24/7 with thousands of gaming machines and hundreds of cameras, even a brief disruption can lead to millions in lost revenue, regulatory violations, and lasting reputational damage.

Yet despite these high stakes, many surveillance infrastructures are still built on traditional architectures that were never designed to withstand catastrophic failure. A single incident—whether environmental, mechanical, or human—can bring down an entire system, leaving operators with no recovery window and no margin for error.

This raises a critical question: what happens when failure is no longer a possibility—but an inevitability?

For one *West Coast casino, that question was answered in real time. Just a few months after implementing a Hyper-Converged Infrastructure (HCI) platform powered by Mirasys, a catastrophic event struck the core of their surveillance environment. What would have forced an immediate shutdown under a traditional system instead became a defining moment—proving that with the right architecture, failure doesn't have to mean collapse.



**Due to the sensitive nature of this story, the casino team requested this to be a blind case study; however, they offered to speak to other IT and Surveillance executives who want to hear the first-hand account of the incident and the solution. Please reach out to your Mirasys sales rep for a private introduction. Thank you for your discretion.*





Executive Summary



Property

Casino Resort on the West Coast

1,000+ Slot Machines
Bingo Hall
Hotel & Restaurants
Bars
500+ Cameras



Area

The Main Distribution Frame (MDF) - A Central Area for the Network, Telephones. The VMS System and recording servers



Incident

An accidental cooling line break caused oily water to spray directly into multiple key business server racks, including the Mirasys VMS platform.

This case study highlights how a modern surveillance infrastructure solution proved its value under extreme, real-world conditions. In highly regulated environments where system uptime is mission-critical, even a brief disruption can trigger operational shutdowns, financial losses, and compliance risks.

When a **catastrophic infrastructure failure** struck a live surveillance environment, the organization faced a scenario that would typically result in a complete system outage. However, due to the implementation of a resilient, hyper-converged architecture, critical systems remained operational despite the incident. This ensured continuous compliance, uninterrupted operations, and avoided significant financial and reputational impact.

Ultimately, this example demonstrates how investing in fault-tolerant infrastructure is not just a technical upgrade—it is a strategic safeguard that delivers measurable value when it matters most.





The Incident

The Catastrophe: When Everything Went Wrong at Once

Shortly after opening the new casino resort property, the surveillance team faced an unexpected disaster.

During a routine test, an anomaly occurred within the CRAC (Computer Room Air Conditioner) system. A cooling line ruptured inside the MDF room, releasing a high-pressure stream of oily water directly into server racks housing core surveillance infrastructure.

The impact was immediate:

- Servers were hit directly by the spray
- Camera streams failed
- The video wall went down
- Operators lost visibility

Under regulatory compliance rules, a complete surveillance outage requires an immediate casino closure.

“There is no grace period,” the Casino Surveillance Manager (CSM) explained. “If surveillance goes fully dark, the casino goes dark.”

The CSM recalled the moment vividly:

“That’s the moment you realize—this could be it. This is how careers end.”





A Critical Decision



The Decision Made a Few Months Earlier—That Changed Everything

Just months before the incident, the CSM had pushed for an investment in Hyper-Converged Infrastructure—despite not being a deep technical expert.

“I didn’t fully understand all the technical aspects of HCI,” the CSM admitted.

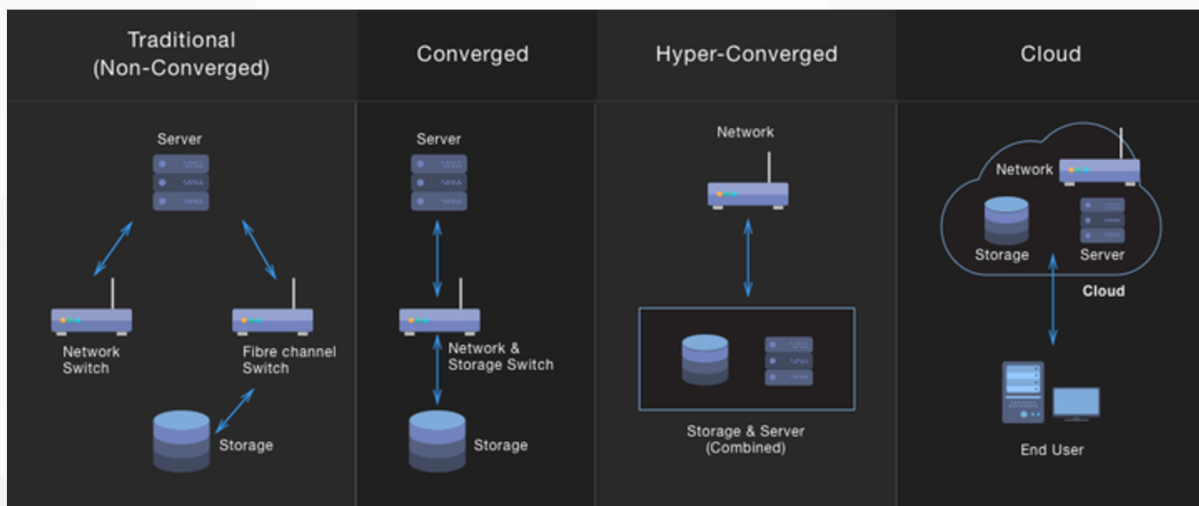
“But I never felt like Max Davis at Mirasys was upselling us to make extra money. I trusted him. I trusted Kellie Vogel. I knew they believed this was the right solution.”

The HCI deployment included:

- 5 independent clusters
- Automatic failover
- Node isolation
- No single point of failure
- Rapid service restoration



Clusters were intentionally located in separate adjacent areas—a decision that would prove critical.





The Casino Stayed Open

When water destroyed multiple servers, entire clusters located outside the spray zone remained operational.

Had the casino been running a traditional architecture:

- The system would have **been completely lost**
- **Full surveillance outage** would have occurred
- The Gaming Commission would have **required an immediate shutdown**

Instead:

- The system limped but **lived**
- Cameras came **back online quickly**
- Core surveillance **remained operational**
- Regulatory **compliance was maintained**

The casino stayed open!

According to the IT Director:

"Without HCI, we absolutely would have shut down. No question."



05 | Research Proposal



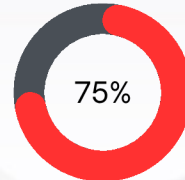
Financial Impact

The Cost of Failure That Never Happened



Hourly Revenue

\$20,000 Per Hour is the Revenue that could be lost should a casino of this size be closed. Being open 24 hours a day equates to **\$480,000** in losses each day a closure is sustained.



Recovery Time

According to the operations team, if the HCI system was not in place, it could have caused them to remain closed for up to **three weeks**. This is due to data server logistical issues.



Revenue (3 Weeks)

If a casino of this size were to be closed for 20+ days, the impact would be hard to recover from. **\$9.6M in gaming revenue would be lost**, which does not include impact to retail, F&B and Hotel revenue.

Beyond The Obvious Financial Loss

- Regulatory penalties
- Loss of patron confidence
- Long-term damage to the casino's reputation and share of wallet



"If we didn't have those clusters, I would've had to make the walk nobody wants to make—the walk up the hill to tell management we had to shut the casino down. That's the walk of no return."

Casino Surveillance Manager





The Human Element



During the interview, the Casino Surveillance Manager underscored the importance of the support team, noting that their response during the catastrophe was pivotal to maintaining confidence and driving recovery. Here's what he had to say:



Surveillance Systems Integration

The CSM praised the President, **Todd Flowers**, and Vice President, **Melissa Mount** unequivocally:



"Todd and Melissa went out of their way to make sure we got what we needed. They are absolute rock stars."



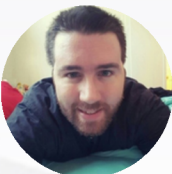
Kellie Vogel (SSI)

Recognized internally as the trusted advisor who helped guide the decision to move forward with the HCI solution. *"Kellie is always there for me and gives me great advice. She is a person I trust."*



Max Davis (Mirasys)

Recognized as a thought leader in the security systems space – *"Max is the smartest guy in this business. He has made me look good so many times, especially when there was a lot on the line. He is my guy, he is the one I turn to when things are challenging, and he always has the right answers."*



Kevin Milne (Mirasys)

Recognized as a team player who stepped up to make the system whole once again while HCI kept the casino open.

"Kevin stayed with us all weekend. He didn't disappear. He fought through it with us until we were whole again. He is Superman in our eyes."





In Conclusion

A Word from Mirasys Engineering

Max Davis, representing Mirasys engineering leadership, reflected on the outcome:

"The Casino Surveillance Manager in this case was an absolute pioneer of HCI. We knew how powerful the solution was—with hardware from VidIO Systems, HCI software from Scale Computing, and installation expertise from SSI. But it always comes down to trust. You have to trust the system—and trust that when something goes wrong, your manufacturer and integrator will fight through the storm with you."

The Bottom Line

This casino did not survive because it got lucky.

It survived because:

- The right architecture was chosen
- The right partners were trusted
- The system was designed for failure, not perfection

Without HCI, the outcome would have been unavoidable:

- Full surveillance loss
- Regulatory shutdown
- Massive financial and reputational damage

Instead, Mirasys, SSI, and the casino's leadership delivered on every promise made.

Final Thoughts

- Catastrophic failures don't announce themselves.
- They arrive uninvited—often during routine tests.
- The only question is whether your surveillance system is built to survive them.

Next Steps:

Access Your Surveillance Risk.

Understand what happens *before* you're forced to make the walk of no return.

