COMPUTER SOLUTIONS INCORPORATED

Cloud Disaster Recovery Case Study

Business continuity through a simulated total site loss



Cloud infrastructure supporting temporary business operations | Illustrative image

Recovery that kept the business working

Computer Solutions, Inc. moved a manufacturing company's critical server services into the cloud, established secure access from an alternate command center, and sustained operations for several weeks. We then restored the environment to replacement physical hardware and verified that staff could use the recovered onsite systems.

Cloud server activation, configuration, and initial verification were completed in under one hour. The return to onsite infrastructure used scheduled downtime to avoid interrupting the customer's normal operations. Written runbooks and verification steps supported the work from activation through final restoration.

The exercise simulated the total loss of the primary location. The server recoveries, VPN deployment, weeks of cloud operation, troubleshooting, and return to replacement equipment were performed in practice.

Client profile Manufacturing company | More than 50 employees and contractors | Monthly revenue exceeding $1.5 million

The continuity challenge

The client operates a demanding manufacturing business where timely responses and reliable access to information support daily activities. More than 50 employees and contractors work within the organization, and monthly revenue exceeds $1.5 million. Live answering, incoming customer requests, and fulfillment are high priorities. The customer’s name and identifying details are withheld.

A major storm could make the primary location inaccessible and leave its physical server equipment unusable. The business would still need access to user accounts and shared information while arranging temporary workspace and replacing damaged infrastructure. The recovery exercise tested how Computer Solutions could establish that continuity and manage the environment until onsite systems were available again.

Defining the environment

The existing environment used a physical Microsoft Hyper-V host running two virtual Windows servers. The DOM server provided Active Directory and DNS, supporting user authentication and the ability to find network resources by name. A separate file server provided shared business files. These services needed to work together for office users to regain practical access.

Our scope followed the complete recovery cycle: bring the protected servers online in the cloud, connect an alternate working location, operate there for an extended period, protect the changes made during that time, and restore the services to replacement physical infrastructure.

Preparing people and procedures

During storm activity affecting Florida’s Gulf Coast, we used the threat as the trigger for a controlled scenario in which the customer’s location was assumed lost. Staff were instructed to take their office laptops with them. Keeping familiar work devices available was part of the continuity plan alongside the server recovery.

We prepared runbooks covering the server environment, network changes, VPN configuration, service dependencies, and restoration sequence. Verification steps gave technicians specific checks to complete at each stage. This reduced reliance on memory and helped distinguish a server that had started from an environment that users could actually use.

Preparation also addressed the eventual return. Cloud operation was a temporary production arrangement, so the work performed there needed to be protected and carried forward when the customer moved back to onsite systems.

Establishing the cloud office



An alternate workspace for coordinating business continuity | Illustrative image

Computer Solutions activated the protected domain controller and file server in CSI's cloud recovery environment. The two virtual machines supported temporary operations, allowing recovery work at a physical location to proceed separately from access to the server services.

Cloud activation, configuration, and initial verification were completed in under one hour. This result applied to the activation stage of the exercise; the subsequent cloud operating period, troubleshooting, and onsite restoration took place over the following weeks.

Linking the command center and cloud environment

We established an alternate command center and deployed a secure site-to-site VPN using a UniFi Dream Machine Pro gateway. The encrypted connection linked the command center network to the cloud recovery network. Staff could reach the recovered services from the alternate working location while the servers operated remotely.

We verified more than the VPN connection itself. Initial checks showed that reaching servers by IP address did not automatically restore access by name or to shared folders. We addressed gateway filtering and DNS settings, adjusted network configuration, and checked domain and file access across the connection.

That troubleshooting was essential to continuity. Staff needed working sign-ins and access to shared information, and our verification steps tested those dependencies. We incorporated the findings into the runbooks to make the recovery sequence more repeatable and efficient.

Managing operations in the cloud

The servers remained in the cloud for several weeks. This extended operating period demonstrated the ability to continue using the recovered services while replacement infrastructure was prepared. In a total-loss scenario, that period would give the business time to arrange a working location and replacement equipment without waiting for the original server host to be repaired.

Computer Solutions managed the cloud environment during this period and continued backup activity. Business information changes after a recovery begins. Protecting those changes was part of the exercise so the eventual return to physical hardware could include the work performed while the servers were hosted in the cloud.

Resolving a backup interruption

The exercise exposed a real interruption in backup activity on a cloud-hosted server. The server continued operating, but its backup process stopped completing successfully. Restarting the affected server resolved the immediate issue, and backup activity resumed. The underlying cause was not confirmed.

This experience tested our response to a complication within the recovery environment itself. The team had to restore backup operation while managing the cloud systems and preparing the return to onsite infrastructure. The runbooks captured the need to verify backup completion during cloud operation, as well as server availability.

Verifying and repairing a damaged disk condition

We also simulated a damaged drive condition and performed disk verification and repair. Several files on one server required repair. This added a recovery complication that had to be addressed before the server could be considered ready for normal use.

Including disk verification helped test the recovery beyond a successful boot. A restored machine can start and still require attention to its files or services. The exercise included those checks so repair work could be completed and the recovered environment assessed before the final transition.

Turning findings into repeatable steps

The runbooks brought together the configuration work and the lessons from troubleshooting. They covered the network connection, domain and DNS dependencies, backup checks, and the order of restoration. Verification at each stage helped the team identify issues before moving to the next stage.

For the customer, the value was a managed operating period while the recovery continued. For Computer Solutions, the exercise provided practical evidence of the work required to sustain the cloud environment and return it successfully to physical infrastructure.

Restoring the physical environment



Server restoration and preparation of replacement infrastructure | Illustrative image

Computer Solutions restored the workloads to a physical Hyper-V host using dissimilar hardware. This represented the replacement equipment that could be needed if the original host were lost in a disaster. Bare-metal recovery and virtual machine restoration reestablished the two-server environment.

The replacement platform introduced differences in virtual machine and network configuration. We addressed the virtual network adapters and network assignments, restored the required static addressing, and returned the network to its original configuration. The domain controller and file server were then verified together.

Using downtime without interrupting the workday

We scheduled disruptive restoration and cutover steps around the customer's available downtime. That allowed technical work to proceed outside normal operating activity and avoided interrupting the customer's workday. Cloud and local server instances were managed during the transition to avoid competing copies of the same production servers.

After the local virtual machines were running, we checked DNS, Active Directory, shared resources, and workstation connectivity. A workstation was tested to verify access to the restored environment. Successful onsite verification completed the recovery cycle and allowed the temporary cloud office to be retired.

The outcome was a return to the original operating arrangement: a physical Hyper-V host, two virtual Windows servers, and the restored local network configuration, with user access verified.

Results of the recovery exercise

Measure	Result in this exercise
Initial cloud activation	Under one hour, including configuration and initial verification
Alternate location access	Secure VPN connection to recovered domain and file services
Extended cloud operation	Several weeks of active operation while onsite recovery was prepared
Recovery complications	Cloud backup interruption resolved; disk verification and file repairs performed
Replacement equipment	Two virtual servers recovered to dissimilar physical Hyper-V hardware
Return to normal operation	Original network configuration restored and workstation access verified
Customer impact	Planned downtime used to avoid interrupting normal customer operations

What this means for your organization

This case demonstrates Computer Solutions' ability to execute a recovery plan through the entire transition: activation in the cloud, secure access from an alternate location, ongoing management, and return to replacement equipment. The exercise tested the dependencies between servers, networks, backups, and user access that determine whether staff can continue working.

Manufacturers and fabrication businesses depend on access to information that supports coordination and fulfillment. Medical and dental practices have similar continuity needs, with additional validation required for clinical applications, imaging systems, connected devices, and privacy requirements. Those clinical systems were outside the scope of this manufacturing exercise.

For larger organizations, a temporary cloud environment can provide time to restore a facility and replace equipment while recovered server services remain available. Each organization's plan must account for its applications, connectivity, staffing, and related systems, including telephony and production equipment.

Plan and test with Computer Solutions

Computer Solutions, Inc. provides hands-on recovery expertise across Hyper-V, cloud recovery, secure VPN connectivity, Active Directory, DNS, and backup troubleshooting. We use documented procedures and practical verification to help businesses prepare for a loss of their primary environment.

Contact Computer Solutions, Inc. to discuss a recovery exercise for your organization and identify the systems your team needs to restore first.

This case describes a controlled disaster simulation with actual recovery work. Timings and outcomes reflect this environment and are not a universal recovery guarantee. Photos are AI-generated illustrations and do not depict the customer's facility, equipment, or personnel.