CLOUD ACADEMY —

How cloud services change your disaster recovery plan

Getting data offsite is easier today, but what happens when the Internet isn't there?

ESTHER SCHINDLER - 2/2/2017, 4:30 AM

National Oceanic and Atmospheric Administration

Enlarge / When something disrupts your connectivity, the cloud may not be your friend.

40

Jessica works at a nursing home in rural Nevada. Most of the software upon which the nursing home depends is cloud-based, such as the electronic health records database Jessica consults before she administers medications. "When there's a widespread network outage, we can't access the health records until it is fixed," she says. "My understanding is that there's basically one big cable into the valley, so there's no easy way to have a backup network solution."

Sure, the nursing home has a disaster recovery plan: a local system for printing paper records. But, Janet (same source, but not her real name, either—their desire for anonymity will soon be clear) isn't quite confident in the plan. "I don't believe the system is frequently maintained or tested or that new nursing staff is trained on it," she says. "For that matter, I'm not sure I remember my own password to it."

This situation isn't atypical. It has become ever harder to get work done without an Internet connection. When the office Wi-Fi cuts out for an hour or a telco cable is cut by a fiber-optic-seeking backhoe, we all stumble around helplessly. Whether the disruption is the result of a construction mishap, a large-scale DDOS attack, or a natural disaster when connectivity is lost, everything screeches to a halt.

Cloud Academy

Cloud Bottlenecks: How *Pokémon Go* (and other game dev teams) caught them all

Great app migration takes enterprise "on-prem" applications to the Cloud

SaaS to the max: The limits of shifting from on-site to cloud services

> View more stories

In daily terms, that's an inconvenience. In a larger context, it's a threat to businesses—and sometimes to human lives.

We know we need to pay attention to connectivity. Today, enterprises spend 28 percent of their total enterprise IT budgets on hosting and cloud services, according to a recent 451 Research study. That reality reflects a growing reliance on external sources of infrastructure, application, management, and security services—next year, the number is expected to reach 34 percent.

In other words: if your Internet connection is down, you're hosed. If it's a major event, the company might not survive it. Almost 40 percent of small businesses never reopen their doors following a disaster, according to FEMA.

Traditional corporate disaster recovery programs consider primarily on-premise problems, such as power outages, server failures, and data loss. These days, disaster recovery plans ought to (but frequently do not) include situations where you can't rely on *any* kind of connectivity to the Internet. Even when the company has a plan to address each element that can go wrong, organizations rarely test those scenarios to make sure the backup actually works—such as, perhaps, ensuring that the nursing staff knows how to access a local system to print paper records.

Want to be prepared? Here are the issues to consider in disaster planning for cloud network outages, whether your problem is a short-term technical mishap (just type in "Comcast outage" on trends.google.com) or a disaster such as a fire or flood.

"Work from Home" isn't disaster recovery

Among the general benefits of the cloud is its accessible-from-anywhere capabilities. That universal availability seems like an easy answer for local Internet outages as well. After all, if your office is dark, employees can still get to online applications from a coffee shop or from home offices. So, the theory goes, workers can write a business proposal in Google Docs or make sales calls with the assistance of a cloud-based CRM even if the company's connectivity is broken.

But, Ars Orbital HQ notwithstanding, working from home is often just a short-term stopgap.

The approach may work for some organizations in some scenarios, says Scott Teel, VP of marketing for Agility Recovery. However, home bandwidth easily can be affected by the event that affected the main office location. "Working from home is only a temporary option, and a precarious one at that," says Teel. "What if the same event (hurricane, tornado, earthquake, etc.) knocks out power and connectivity for your employees?" A cloud disaster recovery plan has to anticipate region-wide network outages or events that disrupt utilities (like power) for days on end.

Disaster recovery planning is all about thinking up the worst case scenarios and ensuring you're ready to cope with them. Whether it's a major regional natural disaster like Hurricane Sandy, or smaller, more isolated events, there are three primary ways to fail:

- Ignorance of infrastructure weaknesses (and thus no alternatives in place)
- Reliance on a single point of failure for Internet connectivity
- Failing to test the disaster plan

Assess your weak points

Planning to avoid infrastructure failure starts a lot like any hardcore IT pen-testing: find the weak spots. If you don't know what can go wrong, you can't establish a process for how to deal with it. And it's much easier to identify the business continuity needs ahead of time rather than when everyone is in a frenzy.

"Every business downplays the continuity aspect, telling you, 'We can go a few hours or even a few days without the Internet,'" says Travis Grundke, operations manager at Ashton

Technology Solutions, a Cleveland-based provider of managed IT services. "Then the Internet drops, a core switch fails, or the power is lost—and suddenly, restoring access becomes an immediate need."

"One of the first things we ask all of our clients is what their pain threshold is for these kinds of events," says Grundke. "We have 100-employee businesses who could operate for days without the Internet or internal network, and we have 10-employee operations that would fold after 15 minutes of downtime."

To plan for such situations, suggests J. Colin Petersen, president of JIT Outsource, run a "fire drill" to find out how your team reacts to a connectivity outage and to learn which departments are most affected. "Document who is able to continue to be productive, who needs to get alternative access, and who simply cannot continue," says Petersen. "Include which of your services are cloud dependent or cloud optional."

The cloud doesn't require you to reinvent the continuity-planning wheel. Many existing processes map to cloud computing disaster recovery, even if old-school data centers focused on relocating the humans and the infrastructure.

For example, during Superstorm Sandy, power outages in Manhattan caused one bank's IT staff to invoke its disaster recovery procedures for the data center in Princeton, New Jersey. Even though it wasn't a cloud scenario, the lessons are relevant. The organization had a set standard of disaster recovery procedures to follow that were tested quarterly, explains Rich Ford, who was then an Oracle DBA in the organization. The details vary with cloud applications, but your company's operational readiness should not.

Additionally, you don't have to go it alone, particularly in large-scale disasters. One example is the Network Centric Operations Industry Consortium's Rapid Response Capability (NRRC). Its goal is to ensure an open process to facilitate cross-domain interoperability and secure information, with a common understanding of what it means to be net-centric sharing. The NRRC details how to create and manage a federated cloud wrapped with a security environment in which all parties can share data, while retaining control of their sensitive and/or proprietary information.

Page: 1 2 Next →

READER COMMENTS 40 SHARE THIS STORY

← PREVIOUS STORY NEXT STORY →

Related Stories

Today on Ars

RSS FEEDS CONTACT US
VIEW MOBILE SITE STAFF
VISIT ARS TECHNICA UK ADVERTISE WITH US
ABOUT US REPRINTS