Jumpstart your Disaster Recovery and Remote Work Strategy:

6 Considerations for your Virtual Desktops

Economic losses from 409 total natural disasters exceeded $232 billion USD in 2019 and closed the costliest decade yet, according to a new Aon (global professional services firm) report, Weather, Climate & Catastrophe Insight: 2019 Annual Report. Of the damages, only $71 billion was insured, so one can't help but wonder if a portion of these economic losses could have been prevented?

What is Disaster Recovery and why is it important?

Business continuity can take many forms. Whether it be a bank processing transactions without interruptions, a retail store transacting sales at point of sale terminals, universities running computer labs with zero downtime, or allowing employees in your organization to work from home seamlessly, business continuity is important to every type of organization. Downtime can result in significant losses in revenue or permanent damage to a brand's reputation. And for those reasons, maintaining employee productivity and access to readily-available computing resources means all the difference.

409
reported natural disasters in 2019 [1]

$17B
U.S. government budget to spend on cyber security in 2020 [2]

What can cause interruptions in business?

It can often be human error internal to the company. Poor communication, lack of process controls, or even physical accidents within the data center can result in failure or an embarrassing shut down. External causes can come in the form of cyberattacks, network interruptions, power outages, disease outbreaks, and of course, weather systems. We've all seen the physical and structural damage that hurricanes, floods, and fires cause - so why would a disaster recovery plan not be priority?

Regardless of cause, a disaster recovery plan should recognize and mitigate these risks to ensure continuous operations. Man-made, adverse health disruptions, or natural disasters can happen to any organization, so your interest in reading this guide is a good step towards safeguarding your IT infrastructure and employee productivity.

71%
of enterprises experienced a downtime event in the past year [3]

[1] Aon Report, Weather, Climate & Catastrophe Insight: 2019 Annual Report, http://thoughtleadership.aon.com/Documents/20200122-if-natcat2020.pdf?utm_source=ceros&utm_medium=storypage&utm_campaign=natcat20
[2] FY 2020 Cybersecurity Funding - The White House https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf
[3] Cloud Endure: "Disaster Recovery Survey Report 2018" https://info.cloudendure.com/2018-Disaster-Recovery-Survey-Report.html

Why are virtualized environments essential to business continuity?

Virtualized desktop infrastructure (VDI) has become a strategic choice for many IT organizations because it can reduce the burden of desktop management on IT staff, reduce costs, and improve uptime and therefore staff productivity. For these same reasons, VDI is essential to your disaster recovery plan. In addition, your ability to implement redundancy to help prevent downtime from occurring in the first place is improved, and you can easily establish reliable server and virtual desktop backups.

Many organizations use a mix of traditional components and virtualized IT infrastructure. As an example, an organization could install a software client on repurposed PCs for some employees and for others deploy thin clients or zero clients. VDI makes it possible to manage a diverse set of devices such as this, connecting users to centralized computing resources.

We know that virtual environments are not fully immune to disasters or business interruptions. But unlike traditional hardware-based environments, there are numerous cost-effective options that allow you to host data in multiple private data centers or public clouds to protect business continuity. The options to diversify where and how data and applications are stored or accessed does not necessarily need to be privately developed – public clouds can offer strategic advantages too. Whether it be IT infrastructure or end-user devices, both are equally important and made easier to manage with the help of VDI.

Take the next step

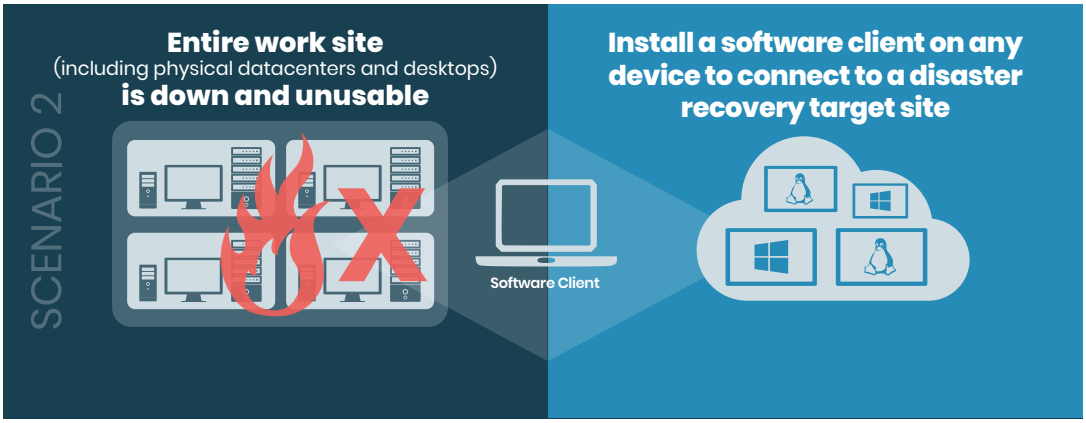
So be proactive and put a plan in place to minimize the impact of a disaster to your business. Planning provides the reassurance that everyone responsible is prepared for when the time comes. Disaster recovery drills—like fire drills or work-from-home test programs—can be conducted periodically to ensure your plan's effectiveness and can be undertaken by staff that will manage operations in the event of a disaster. Even risk assessments can be helpful to determine gaps in a disaster recovery plan. However your approach, be sure to consider the key points in the next section when planning.

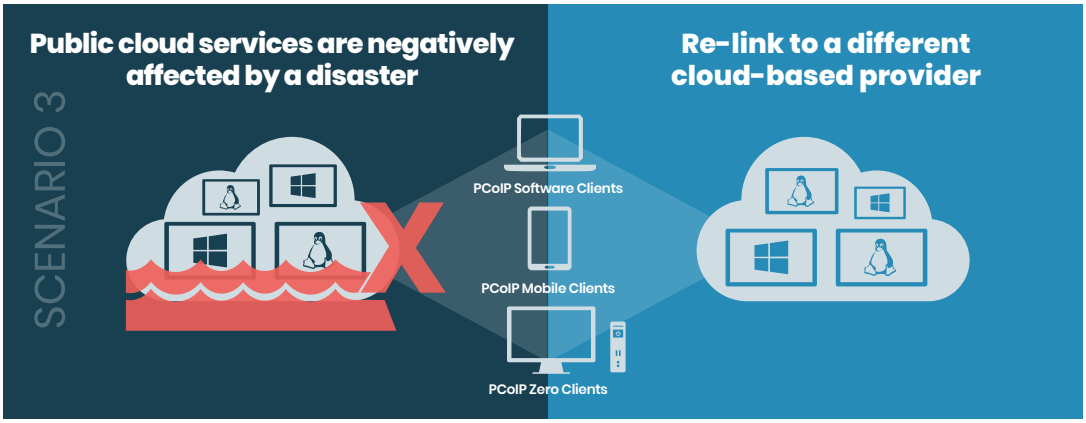
6 considerations to jumpstart your disaster recovery strategy...

1 Leverage existing infrastructure when possible

Leveraging investments in existing infrastructure as part of your disaster recovery or business continuity plan will save costs and time spent training staff. Imagine a scenario where a power and networking issue disables your on-premises data center where your virtual machines are hosted, but physical endpoints and devices such as thin clients or zero clients are functional. Staff can remain working in the office or at home, and use their existing devices to seamlessly connect to a disaster recovery target site.

Should the power outage extend to the office itself, staff may be forced home. In situations like this, disaster recovery solutions that enable remote access should be high on your checklist. Consider options that allow for a lightweight software client to be installed on a home PC or laptop, enabling quick and easy connectivity to a disaster recovery target site. This will empower employees to work from anywhere and offer flexibility even if their offices are inaccessible.

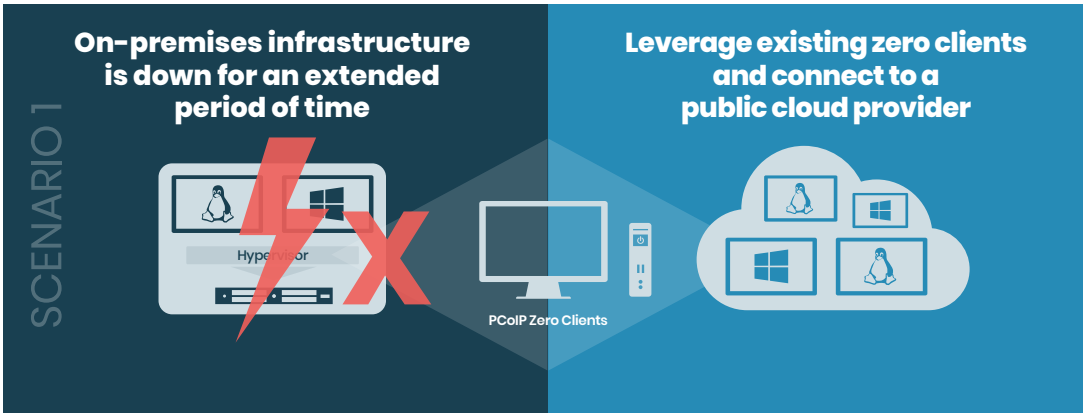




2 Seek multicloud or cloud-agnostic solutions

According to a 2018 CloudEndure survey of 375 IT Professionals around the world, almost half (47%) of all companies surveyed use a public cloud as their disaster recovery target site, while only 15% use physical machines and 39% use private clouds.

A disaster recovery or business continuity plan utilizing public clouds has many benefits. It is less expensive than on-premises recovery sites since you only use resources when needed. There is no need to invest in infrastructure that may never be used, not to mention the real estate or related capital expenditures. Additionally, for global organizations, multiple disaster recovery sites may be mandated by company policies or industry regulations. Public clouds are confidently reliable, much simpler to set up, and generally have a service level uptime of 99.9% – so why wouldn't you consider this?



3 Ensure that a brokering and provisioning service is in place

Once your secondary computing resources (i.e. your virtual desktops), are established in multiple clouds, it is vital to have a brokering and provisioning service that communicates to all virtual desktops. To clarify, look for a management service that manages users, virtual machine entitlement, usage, and the automation of new virtual desktops when needed. In the event of a disaster, business interruptions, or any time for that matter, provisioning additional virtual desktops is much faster and more efficient than provisioning physical desktops. Brokering is also important when the primary site is down for an extended period of time. With the right solution, IT can leverage functions like auto-detect brokering and load balancing to simplify the process employees go through to access their virtual desktops. For example, IT can put rules in place that automatically direct employees to where they should access their desktop in the event of a disaster - employees can simply continue to work and be productive.

4 Turn virtual machines on/off for costs savings

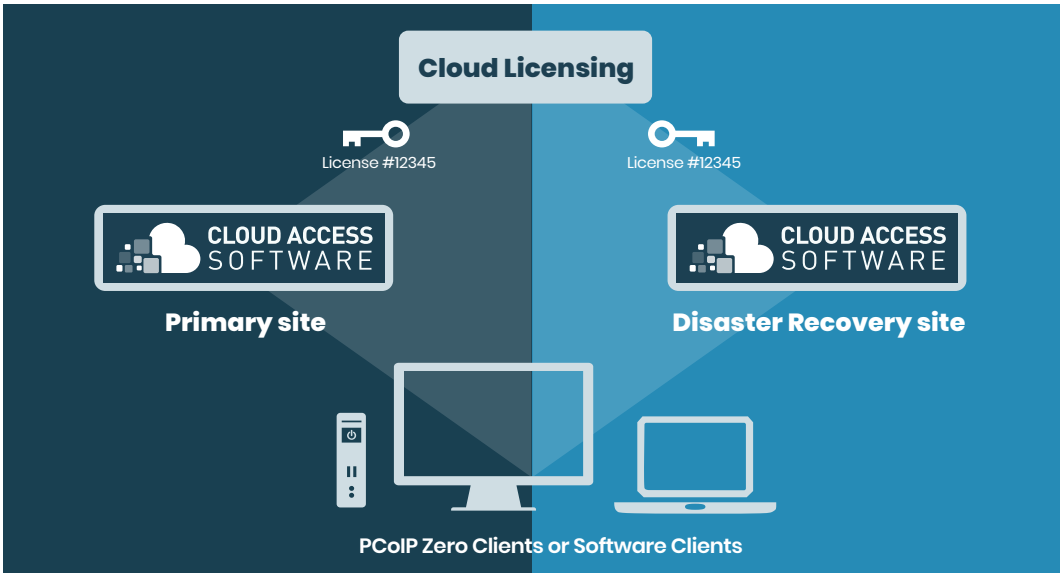
Most public cloud providers provide hourly and monthly usage options . “Pay per use” consumption billing allows for greater control over costs - just pay for the cloud only when in use. In other words, virtual desktops that use the public cloud will be billed. So having a service that turns these machines on and off is extremely useful for forecasting and managing your disaster recovery or business continuity expenditures. Employees working from home can control the number of hours that they need access to their virtual machines.

5 Ask if cloud licensing is in place

Cloud licensing goes hand in hand with the ability to turn virtual machines on and off. With concurrent licensing and cloud licensing, make sure you can transfer licenses from your primary site to your recovery site (an additional way to reap cost savings). If you need to add additional licenses for your disaster recovery site, this is simple to set-up and add. In the case of work from home scenarios, the licenses you utilize can seamlessly transfer, rather remain consistent, no matter where your staff are located. Adding licenses for employees who first start to work from home is a simple and headache-free process.

Cloud licensing avoids the need to deploy and maintain a license server. All licenses are concurrent, so customers only need as many licenses as the number of concurrent logins. In order for this to happen, the host desktop must maintain an internet connection directly or through a proxy.

If the host desktop does not have access to the internet, consider license server licensing. License server licensing is typical of dark site environments, where even the license server (or proxy server) does not have internet access.



6 Choose a secure solution that delivers on performance

From the same 2018 CloudEndure survey, 71% of respondents experienced a downtime event of varying magnitudes in the past year. Does this surprise you? It shouldn't. That is why you evaluate solutions that use a remote visualization solution that can:

- Support applications used by knowledge and power users
- Work under varying network conditions
- Offer best-in-class security
- Enable an amazing user experience that allows employees to work productively and seamlessly as if their virtual desktop were attached to their physical desk

PCoIP® technology has long been adopted as a secure remote work solution by customers in many industries such as media and entertainment, engineering and construction, government, finance, healthcare, and education. PCoIP technology secures data by transferring only image information in the form of pixels – so business information never leaves the cloud or data center. From a user's perspective, the computing experience is no different than working with a local computer loaded with software. In fact, it is more high-performing.

Conclusion

IT downtime or unexpected interruptions for your business is inevitable. Whether it be a few minutes or a few hours, the consequences can be very costly. In order for employees to be up and running quickly, it takes a virtual desktop solution that can deliver on ease of use, security, and performance. Ensure your disaster recovery and business continuity plan guarantees the quick recovery of files, applications and virtual machines so you have backup and recovery capabilities in place to meet service level agreements (SLAs) for recovery time and recovery point objectives.

Cloud Access Software from Teradici is a multicloud solution that enables organizations to easily deliver Windows and Linux desktops and applications from any cloud or data center to any device, with full encryption. Built on industry-leading PCoIP technology, it provides the highest user experience and security, and total cloud independence. Included is Cloud Access Manager, a powerful brokering and provisioning service that allows for simple and effective management of all Cloud Access deployments, with the ability to scale as needed.

Get in touch with a Teradici Sales Representative

Book a meeting
teradici.com/kmarkle

Visit
teradici.com/cloud-access-software

teradici®