CLOUD | EBOOK

MITIGATING DISASTER

Keeping your operations flowing with cloud-based business continuity and disaster recovery plans

Hyland®

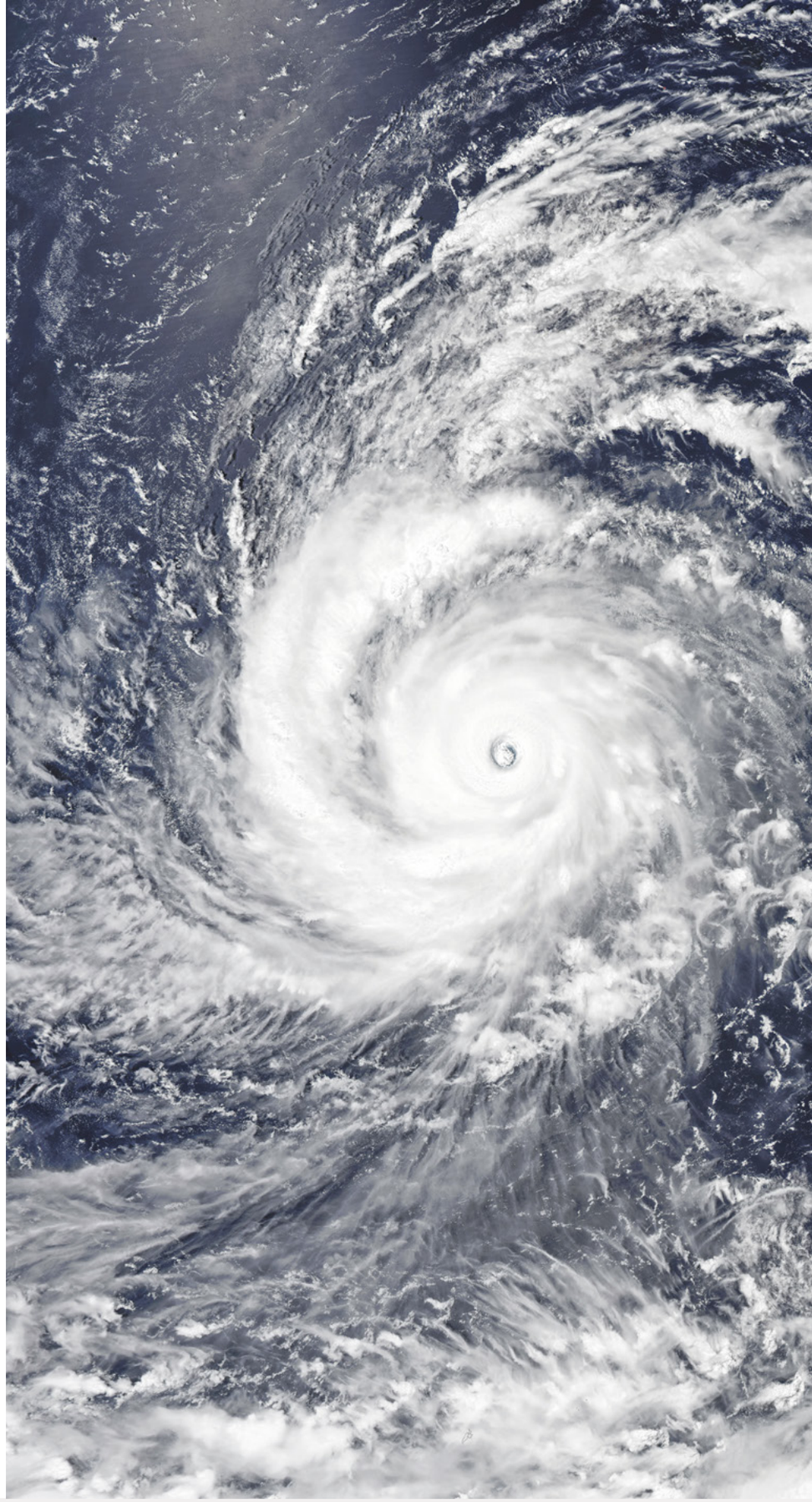
Though it started out as nothing more than a weak system of low pressure churning through the western Caribbean sea in late October 2012, within hours, it became a tropical storm. Two days later, it was a seething hurricane with a name, Sandy, charging toward the United States' eastern seaboard.

Landfall came on Oct. 29 near Atlantic City, New Jersey. By the end, Sandy tore through 24 states, becoming the most destructive hurricane in 2012, causing more than $65 billion in damage[1]. Sandy crushed homes, tore down buildings and flooded entire cities. Roads became impassable. Clean water and power were hard to come by.

The super storm's economic impact went beyond property destruction. It shut down hundreds of businesses, inflicting untold costs in lost data, missing information and diminished customer confidence.

ROM Reinsurance was at the heart of the storm. When Sandy's storm surge washed over Manhattan, it dumped three feet of water in the insurance company's lobby. When the power flickered out, ROM was left in the dark, literally and metaphorically, losing access to critical digital business systems and, with that, the ability to serve clients at the precise moment ROM's customers needed them most.

"We weren't sure how to keep our business running," said Marianne Petillo, president and CEO of ROM Reinsurance.



When it comes to business continuity, even the most developed program can go astray if a raging hurricane — or cybercriminal — finds a flaw in a company's disaster recovery plan. That flaw, for many organizations, is adhering to traditional disaster recovery practices, most notably by hosting digital data and critical software solutions on-premises.

For some, this may sound counterintuitive. Protecting business systems within the confines of an organization allows for multiple safety protocols, from digital firewalls to limiting physical access to company servers, and complete control over those protocols.

Control comes at a cost, however. Maintaining the physical integrity of a server cluster is complex and expensive, around-the-clock security is demanding, and cyberattacks alone can cost the average company $200,000 or more per year[2].

And IT support can fluctuate, which brings us back to ROM Reinsurance.

Prior to Hurricane Sandy, ROM went through an extensive digital transformation, eliminating its reliance on paper and manual processes and embracing sophisticated workflow solutions that boosted productivity and efficiency across the company — all hosted on-premises. But in less than 24 hours, the flaw in ROM's business continuity plan was made clear:

WHAT IF YOU SIMPLY CAN'T GET TO YOUR INFORMATION?

"With three feet of water in the lobby, we were thankful we eliminated paper, but worried because our data and documents were on our IT systems," said Petillo. "And we didn't have access to them."

Thankfully, ROM found a solution. While storm clouds brought the full might of Sandy to ROM's front door, ROM would take its business to the digital cloud, mitigating the business continuity threat of Sandy — and so many other disasters like it — for good.

Almost overnight, managed digital services in the cloud became the most crucial component of ROM's business continuity and disaster recovery plan.

But how? Let's find out.

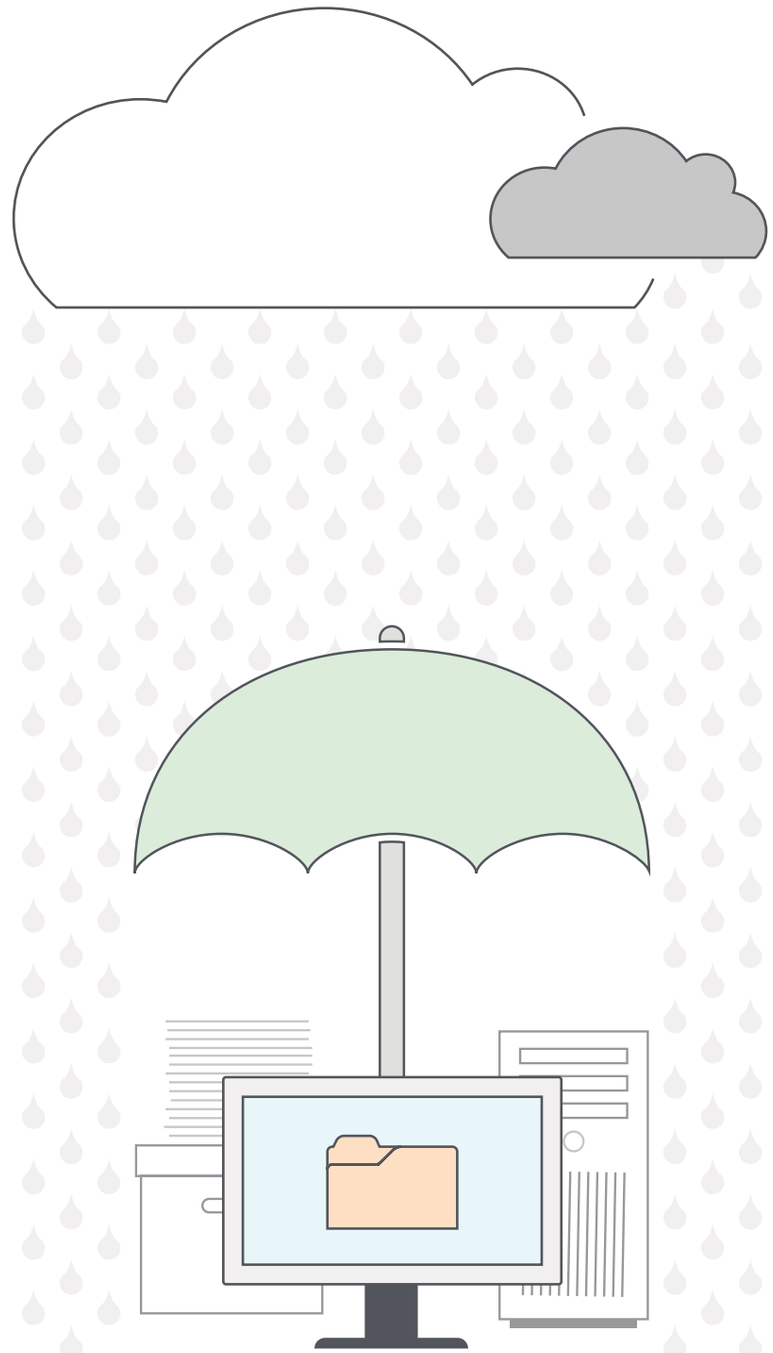
HOW BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS WORK TOGETHER

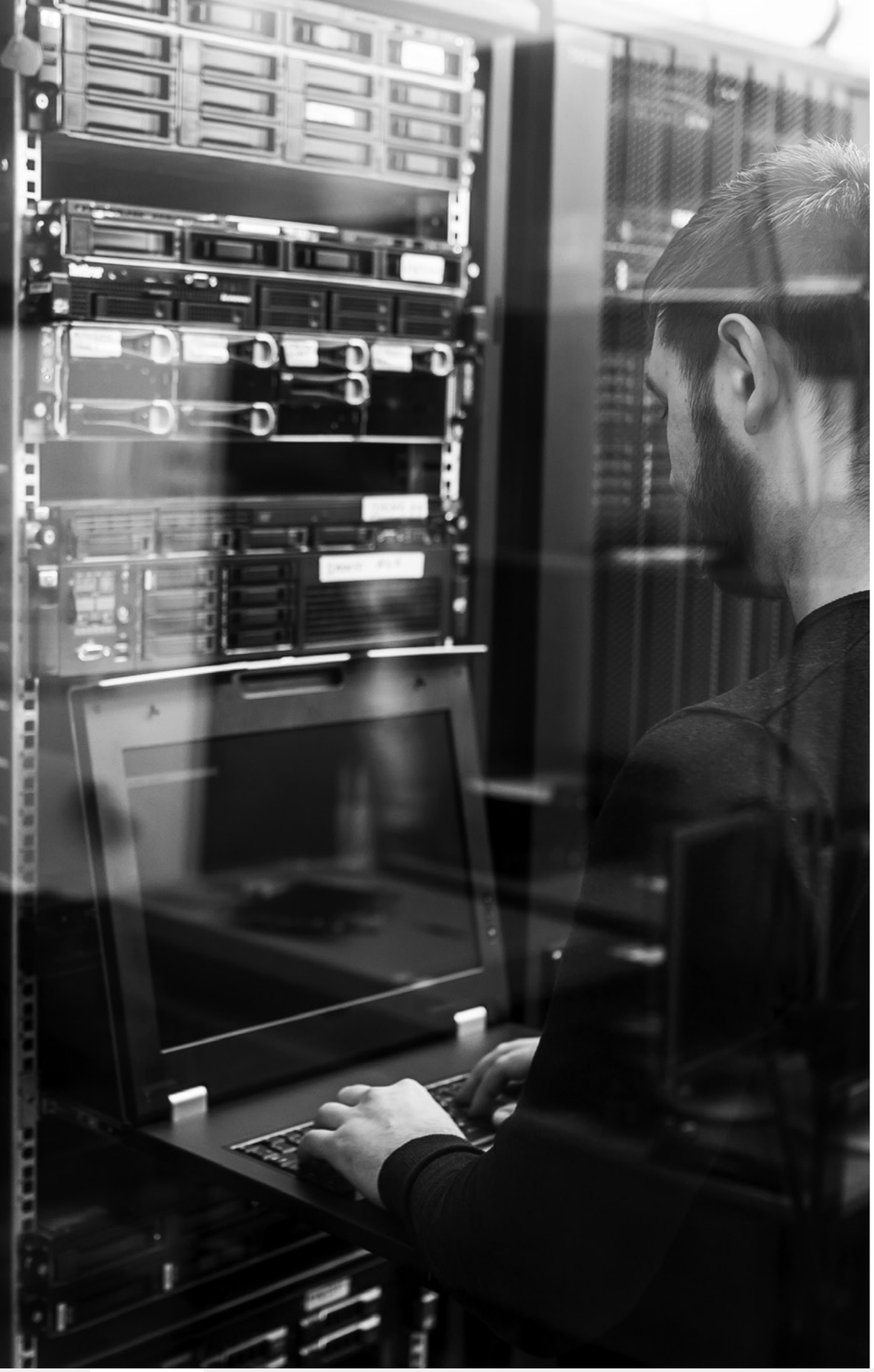
Before diving into how cloud services can transform any organization's business continuity and disaster recovery plans, it is important to understand the concept behind each, as well as how they work together.

WHAT IS A BUSINESS CONTINUITY PLAN?

Think of your business continuity plan as the umbrella that both shields your organization from any potential threat, external or internal, and shines a light on recovery if one of those threats proves successful[3]. The plan protects personnel and assets and provides guidance on how to quickly recover and continue serving customers in the event of a disaster, from fire and flood to software corruption and cybercrime.

Organizations build business continuity plans well before disaster strikes. They build plans upon relentless analysis of business systems and vital input from key stakeholders across the organization. Critical business processes are flagged, resources earmarked for essential services and decisions made regarding how to provide continued service to customers and prospects.





“The impact of data loss or corruption from hardware failure, human error, hacking or malware could be significant. A plan for data backup and restoration of electronic information is essential.”

— THE READY CAMPAIGN
Ready.gov

WHAT IS A DISASTER RECOVERY PLAN?

Disaster recovery plans focus on restoring critical business systems identified in the business continuity plan. In other words, how quickly must your organization restore certain business processes and provide access to critical data needed to serve customers and limit economic damage to the company?

Execution of a well-designed disaster recovery plan, then, is the linchpin to true business continuity. But when the plan relies on access to on-premises technology and the IT staff to service it, including secondary data centers, that can be a wild card. Are both data centers affected? Can staff reach the servers? Is staff available? Do they have the expertise to restore data access?

Disaster recovery plans that rely on on-premises IT resources can become complicated, expensive and susceptible quickly when the unexpected happens.

COURTING DISASTER: **COVID-19**

As the novel coronavirus began to spread throughout the globe in early 2020, organizations across industries, both large and small, found themselves in a predicament. How would they shut down some offices and enable hundreds of thousands of staff to work from home — away from the IT and information infrastructure built on-premises?

This was significantly more complicated for healthcare systems. They had to adapt quickly to protect essential workers and patients, enable a remote workforce that was not accustomed to working from home and ensure the continuity of patient care. Rolling out new technology that would enable access to critical information for remote workers was daunting, if not impossible. For hospitals with on-premises infrastructure, add to that the need to develop safety protocols for employees and vendors who would likely need to be on-site, in-person to manage any implementation or maintenance.

Hosting that technology infrastructure in the cloud, however, would allow healthcare organizations to quickly adopt new technology and implement solutions remotely alongside its vendor partner. In short, an organization that housed its information architecture in the cloud rather than on-premises is ready to scale up at a moment's notice. It doesn't have to worry about placing staff in harm's way to keep the organization running.

That's likely why a majority of healthcare organizations — 65 percent, according to a recent study by HIMSS Analytics — use the cloud or cloud services. After all, of those cloud-enabled providers, 37 percent stated disaster recovery concerns as the primary reason for moving to the cloud, making it the number one driver by far[4].

THE CLOUD: THE MOST CRUCIAL COMPONENT OF YOUR DISASTER PLAN

When we last left ROM Reinsurance, the insurer was knee-deep in storm surge, unable to access the technology it needed to run critical business systems, access information and serve customers — many of whom were relying on ROM to help them through their own disaster recovery.

It is possible many of those organizations also relied on the ability to fail over to a secondary data center in the event staff could access content and business processes stored electronically on-premises. This traditional approach to business continuity and disaster recovery is smart and can be very secure, but only with respect to ongoing maintenance of internal controls and security.

The traditional method also requires management of the secondary facility, one that's large enough to house the right IT infrastructure and the employees to maintain it. Scalability can be difficult, connectivity a challenge and network infrastructure costly. Not to mention the very real possibility that a secondary data center could be susceptible to the same disaster as the on-premises solution.

If that happens, businesses may find themselves stalled, unable to serve customers and not knowing what to do next. It's the situation ROM found itself in before it reached out to its content services platform vendor, Hyland, to see if its experts could offer guidance.

Hyland experts recommended quickly migrating critical business processes and information to the Hyland Cloud. ROM agreed, and with Hyland's help, ROM was back up and running in short order. Employees had access to documents and data to process claims and get much-needed funds into its clients' hands.

COURTING DISASTER: **CYBERCRIME**

Most people think of floods, fires and tornadoes when they hear the term disaster recovery. IT departments, however, almost exclusively think of cybercrime. With only 5 percent of companies' folders properly protected, on average[5], and data breaches exposing 4.1 billion records in the first half of 2019[6], it's easy to see why.

Cybercrime offers a look at business continuity and disaster recovery through a completely new lens. It's an even more important issue now that remote workforces have become a part of our new normal — and a tantalizing target for cyber criminals. As organizations consider moving both information and business processes to a privately managed cloud, they should also consider the digital content services they're investing in.

Because so much confidential data passes through today's business systems, organizations expect modern information management solutions to meet a higher degree of scrutiny when it comes to data security. Modern digital systems and procedures must be fully secure to retain the trust of businesses and customers alike, and to protect companies from liability.

Look for a natively secure platform that keeps information and processes protected at every data state: at rest, in transit and in use. And make sure the system is secure by default, meaning that the most secure option is turn on by default.

LOOKING BEYOND DISASTER RECOVERY

Beyond being the best choice for business continuity and disaster recovery, there are several additional reasons why moving IT to the cloud can elevate your organization. Support and customer service for example.

In other words, the people behind a private cloud — the platform experts — are key to both continuity and company growth. For any organization, access to platform experts means fewer in-house technical resources need to be assigned to monitor, upgrade, patch, procure, troubleshoot and manage software solutions, digital processes and hardware infrastructure. This frees your staff for other innovative and value-add work.

At the same time, IT departments become partners with a team dedicated to security, availability and disaster recovery. The best cloud-based providers have service level agreements, or SLAs, that mandate they address any issues immediately. There is 24/7/365 support in the event of any disruption to service.

And IT leadership can rest easy knowing those experts are working within one of the safest environments possible. Often, the level of security provided by reputable data centers that run private, managed clouds is quite higher than the kind of security an organization could practically provide or afford for itself. Depending on the needs of individual companies, controls include guarded access and mantraps, and can go up to biometric controls and beyond.

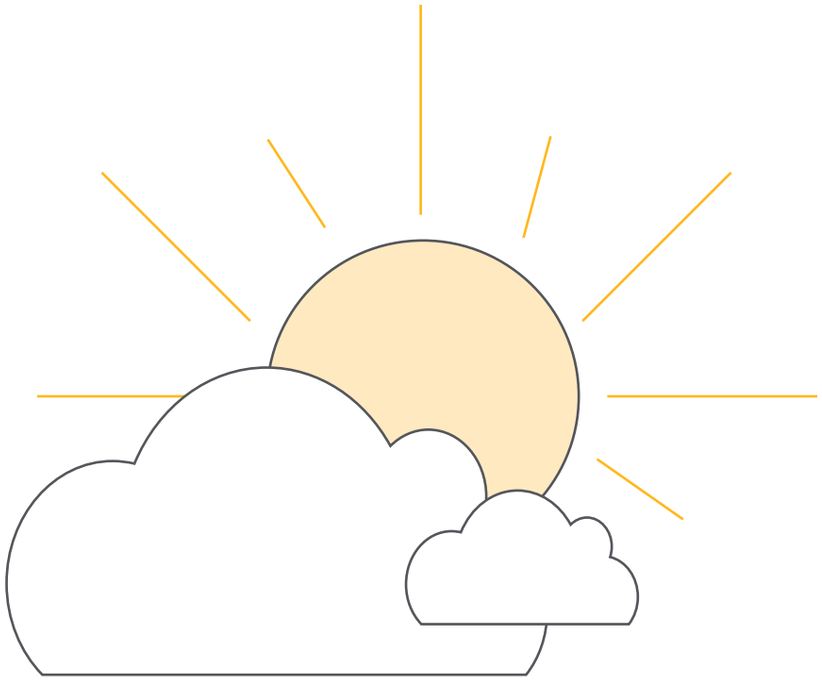
At a time when IS staffing is lean and IT departments are asked to do more with less, this is a huge benefit. Those in-house teams can now dedicate their time to developing innovative solutions that exceed customer expectations and propel the company forward.

CONCLUSION

As communities battle wildfires in the western United States, small businesses cope with a record-breaking hurricane season, and the coronavirus pandemic upends virtually everyone, business continuity and disaster recovery takes on new meaning and increased urgency. Private businesses, government agencies, healthcare systems, higher education institutions and more are all scrambling to ensure they can maintain the flow of patient care and client service by maintaining the flow of critical information to staff.

To do so, those same organizations must re-evaluate the foundation of their disaster recovery plans: Where information is stored, how it is accessed, the cost of maintaining those systems — and whether any kind of disaster can disrupt those plans. Unfortunately, for on-premises systems, the threat of disruption is always there.

From storm surges to data corruption, disasters are unpredictable. Even when we are prepared for one scenario, something complete unexpected is likely to occur. True resilience and disaster recovery is possible, however — when crucial information is stored in the cloud and vital business processes are cloud-based.



SOURCES
1. U.S. News & World Report, The economic impact of Hurricane Sandy, 2012
2. CNBC, Cyberattacks now cost companies $200,000 on average, putting many out of business, 2019
3. Investopedia, Business continuity planning, 2020
4. The Hyland Blog, Healthcare providers can do more in the cloud, 2020
5. Varonis, Varonis Global Data Risk Report, 2019
6. Varonis, 2019 on track to being the “worst year on record” for breach activity, 2019

Hyland®

Learn more at **Hyland.com/Cloud**