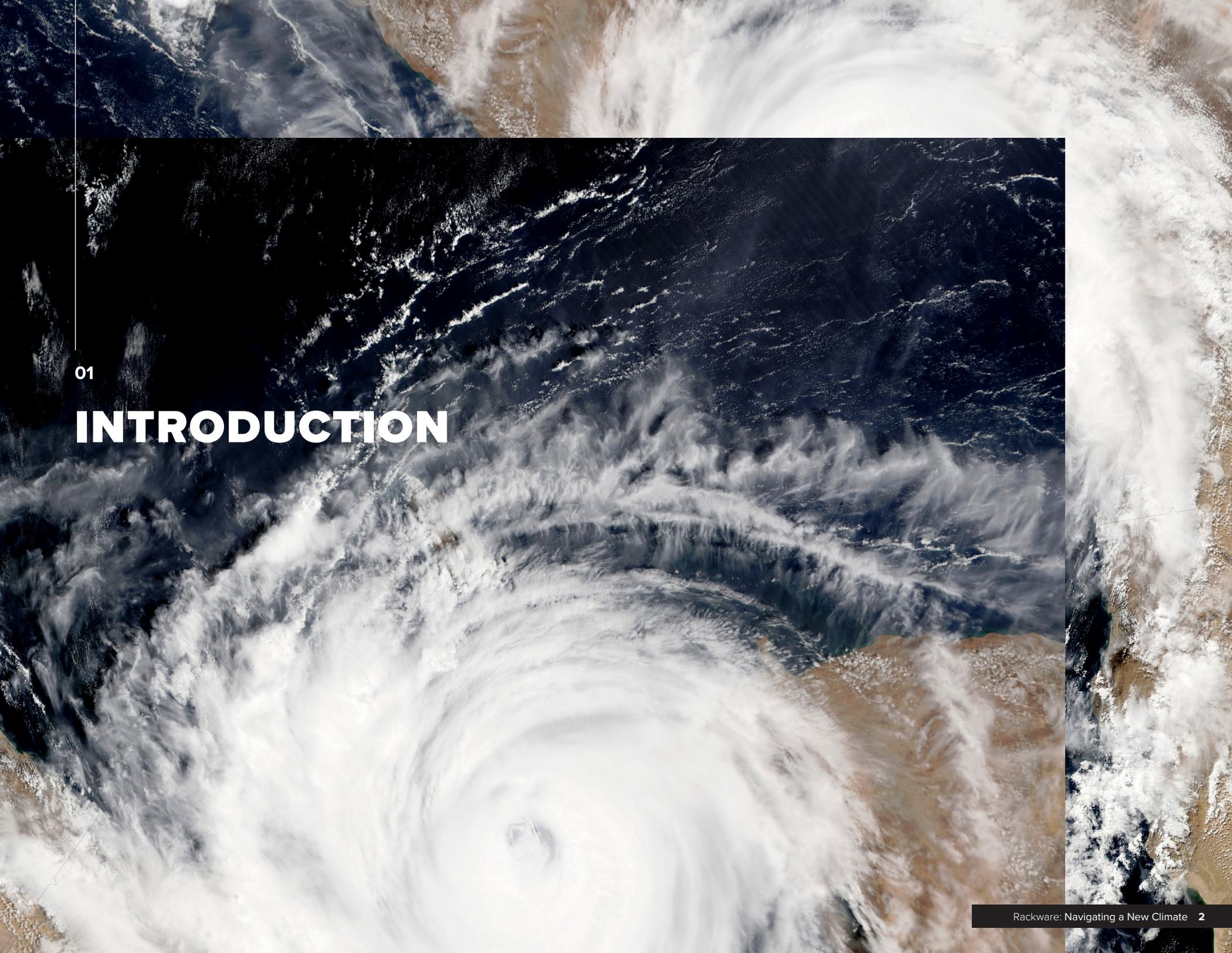


The Rackware logo, featuring the word "Rackware" in a white sans-serif font followed by a blue icon of a cloud with a lightning bolt striking it. The background of the entire image is a dark, stormy sky with a lightning bolt striking down and a road leading into the distance.

Rackware

NAVIGATING A NEW CLIMATE

The impact of extreme weather on business disaster recovery

A satellite image of a tropical cyclone, showing a distinct eye and spiral cloud bands over a dark blue ocean. The image is partially obscured by a vertical white line on the left side.

01

INTRODUCTION

Disaster recovery planning and strategy is a pivotal component of business continuity. As IT leaders know, a business without a disaster recovery plan is like a person without health insurance: When the unexpected happens, the costs accrue quickly and unmanageably.

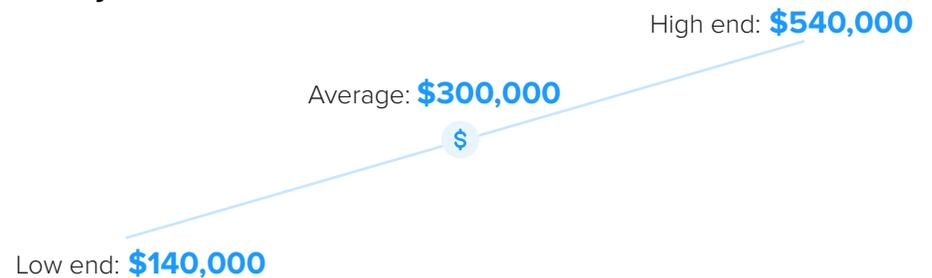
And these costs are not just monetary. Yes, there's the hefty \$5,600 per minute price tag (on average) of IT downtime — which adds up to over \$300,000 per hour.¹ But then there's the intangible impact downtime has on brand perception. Customers have a reasonable assumption of continuous uptime. When that assumption is tested, so is their loyalty.

The average cost of downtime²



\$93 per 1 second = **\$5,600** per 1 minute

Hourly costs of downtime



What you can lose during downtime

-  Customer Trust
-  Brand Loyalty
-  Sales Revenue
-  Employee Productivity
-  Materials
-  Regulatory Adherence

1. <https://www.zdnet.com/article/the-astonishing-hidden-and-personal-costs-of-it-downtime-and-how-predictive-analytics-might-help/>
2. <https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/>, <https://www.dobson.net/much-downtime-really-cost-business/>

Given the importance of disaster recovery to a business' bottom line, it's not surprising that enterprises devote significant time and resources to devising the best lines of defense against downtime. For IT leaders, enterprise resilience means having a business continuity plan that's comprehensive, adaptive and future-focused.

Over the past decade, the enterprise conversation around DR has largely focused on strategies for pivoting away from on-premise-only solutions and toward a hybridized or entirely cloud-based model. But in recent years — and particularly within the last year — an expanding list of high-profile weather events have brought a new obstacle to the forefront of DR planning: The impact of extreme weather.

2018's Top 5 \$1 billion+ disasters³

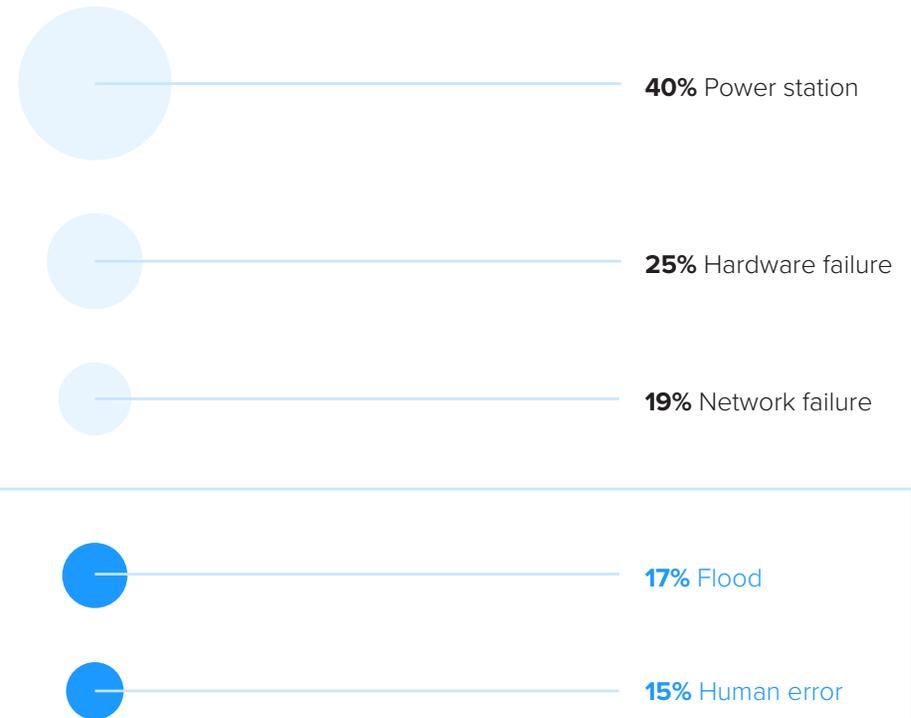
	Hurricane Michael, FL	\$25,000,000,000
	Western wildfires, CA	\$24,000,000,000
	Hurricane Florence, NC, SC	\$24,000,000,000
	Northeast winter storm, MD, MA, NH, NJ, NY, PA, CT, DE, RI, VA	\$2,200,000,000
	Hail storm, CO, UT	\$2,200,000,000

3. <https://www.ncdc.noaa.gov/billions/events/US/1980-2018>

In 2018, a series of extreme weather incidents starkly highlighted the tragic, disruptive and costly impact of major climate shifts.⁴ Hurricane Michael, for instance, was the most powerful hurricane ever to make landfall on the Florida panhandle.⁵ Meanwhile, California experienced the most devastating and tragic wildfires in the state's history, which killed 87 people.⁶ Besides the tragic human costs, these weather events incurred huge monetary costs as well, with businesses significantly impacted.

For enterprise disaster recovery leaders, major weather events present new and unique challenges to safeguarding mission-critical data. And as extreme weather worsens — which climate experts warn to expect — having the disaster recovery infrastructure in place to withstand these conditions will be a business imperative.⁷

Top 5 reasons behind enterprise downtime⁸



A flood is more likely to cause downtime than human error.

4. <https://www.cfr.org/article/year-extreme-weather-climate-2018> 5. <https://www.cnn.com/2018/10/10/us/hurricane-michael-dangers/index.html>
6. <https://abcnews.go.com/US/relentless-california-wildfires-leave-87-dead-600-unaccounted/story?id=59262994>
7. <https://www.nbcnews.com/health/health-news/climate-change-going-make-life-earth-whole-lot-worse-report-n938101>
8. <https://www.10gea.org/articles/disaster-recovery-cost-of-downtime/>



02

THE UNIQUE DISASTER RECOVERY CHALLENGES POSED BY EXTREME WEATHER

While most enterprise technology leaders are familiar with the hurdles they face in DR planning, extreme weather events introduce some new challenges into the mix, including:



The infeasibility of traditional infrastructure

More than anything, extreme weather events like the fires in California highlight the damaging — and possibly business-ending — limitations of traditional backup methods, especially a geographically contained infrastructure. Say, for instance, a California-based company decided for the sake of travel convenience to house its entire data infrastructure at data centers exclusively in the region. **In this situation, that business could have faced significant — and potentially untenable — downtime during the fires as a result of mass evacuations.**⁹

A greater need for cloudware

Beyond revealing traditional data infrastructures' limitations, **extreme weather points to a greater need for both cloudware and, within physical data infrastructure, secondary power sources. These are vital lines of defense against potentially business-ending downtime.** Unfortunately, many businesses — particularly smaller enterprises — don't realize the critical need for the on-demand resources the cloud provides until their primarily on-prem infrastructure is compromised, as happens during major weather events. Without leveraging cloud-based solutions to some degree, businesses will find it very challenging to fulfill their RPO and RTO in a major weather event, jeopardizing mission-critical data and putting client relationships at risk.

Communicative excellence

Finally, events like Hurricane Florence and the California fires will inevitably reveal the cracks in business' organizational and communicative frameworks surrounding DR. If a business' DR strategy isn't being managed with the appropriate considerations on all fronts — including acceptable RPOs and RTOs; adherence to customer SLAs; and planning for company growth — then they will experience even more downtime in the event of a natural disaster. Similarly, **if there are communicative shortcomings in a business' DR planning — such as inadequate business continuity planning between separate locations — a major weather event will not only highlight, but also compound the negative impact of, these shortcomings.**

⁹ <https://www.fastcompany.com/90265387/heres-the-latest-on-the-california-wildfire-evacuations>

03

THE 3 PROACTIVE STEPS TO MITIGATE THE IMPACT OF EXTREME WEATHER

Despite the formidable challenges extreme weather poses to DR — and the potentially significant degree to which these weather events may test existing approaches — there are key proactive steps enterprises can take to level up their existing DR strategies for a more disaster-prone climate. Here are the three most important moves businesses should make to proactively prepare for evolving climate threats:



Invest in cloudware and adaptive management

If businesses had any doubts about the necessity of investing in both cloudware and the tools to effectively manage a hybrid cloud platform, the increase in extreme weather events should put those doubts to rest. As events like the California wildfires and hurricanes Michael and Florence have highlighted, the unpredictability and scale of destructive weather events places an urgent imperative on businesses of all sizes to prioritize IT resiliency.

In practice, that means having both an adaptable DR infrastructure and an intelligent solution that limits the complexity and costs associated with managing this infrastructure.

ZS Associates is one example of a company that sought such a solution.¹⁰ As one of the biggest enterprise service firms in

the world, the business needed a tool that would both scale alongside the company's rapid growth and keep downtime to an absolute minimum. And, with a data center environment that was divided between Chicago and New Jersey, ZS Associates needed a solution that could easily accommodate a geographically-dispersed network.

The solution they turned to was the RackWare Management Model (RMM), a platform that can work across virtualized and bare-metal physical infrastructures to deliver out-of-the-box maintenance of business-critical environments. In the case of ZS Associates, **the adaptive management RMM helped the company bring its downtime reduction and failover capabilities to the next level. Other companies can look to solutions like this for the adaptive management that today's business climate demands — particularly with the rise in natural disasters.**

10. <https://www.rackwareinc.com/zs-associates>



Improve RTOs and RPOs

Businesses can't prepare for the specific nature of a disaster, the breadth of its impact, or the time it will take to subside. But they can control their response — specifically, their recovery point objective (RPO) and recovery time objective (RTO). But RTOs and RPOs aren't something to solidify and then sideline. On the contrary, they are standards that need to be continuously evaluated and evolved as industry changes — and, yes, climate changes — demand.

However, in order to approach RTOs and RPOs with an eye to adaptiveness and efficiency, enterprises need a solution provider that accommodates these goals. For ZS Associates, RackWare was that provider, offering ZS the capability to customize RTO and RPO according to their evolving needs.

As Mark Kocour, Associate Principal, Global IT at ZS Associates, noted, “We easily implemented and improved our disaster recovery strategy without buying additional hardware. We can now protect a larger number of workloads across our data center while increasing their availability. RackWare allows us to reduce downtime during an outage, with failover capabilities of complex and expensive high-availability solutions, but at a fraction of the cost.”



Have the right team in place

While solutions like RMM can play a transformative role in enabling companies to meet evolving DR demands, an enterprise's DR work doesn't end with the right solution provider. **Effective planning and team preparedness is also a key part of the equation. And on this front, it's important to make sure that the responsibility of DR isn't a siloed function within IT.** Instead, business continuity planning — including disaster recovery — should reflect a collaborative process across IT managers, business owners of apps, and technical owners of apps.



The Takeaway

If 2018 was a notable and even precedent-setting year in terms of extreme weather, 2019 promises to bring more of the same. According to this year's Global Risks Report — an output of The World Economic Forum — extreme weather and climate catastrophe are among the biggest threats to global prosperity.¹¹

Reading the report, there's one term that recurs within the discussion of extreme weather: Resilience. As the report asserts, extreme weather will test our collective resilience, including the existing infrastructure we have in place.

For business technology leaders, resilience should also be top of mind when it comes to managing robust DR strategies in the face of increasingly unpredictable weather events. The most important step toward achieving that resilience is to partner with a solution provider that improves RPO/RTO, offers support across all applications, and delivers compatibility across physical, cloud-based and hybridized environments.