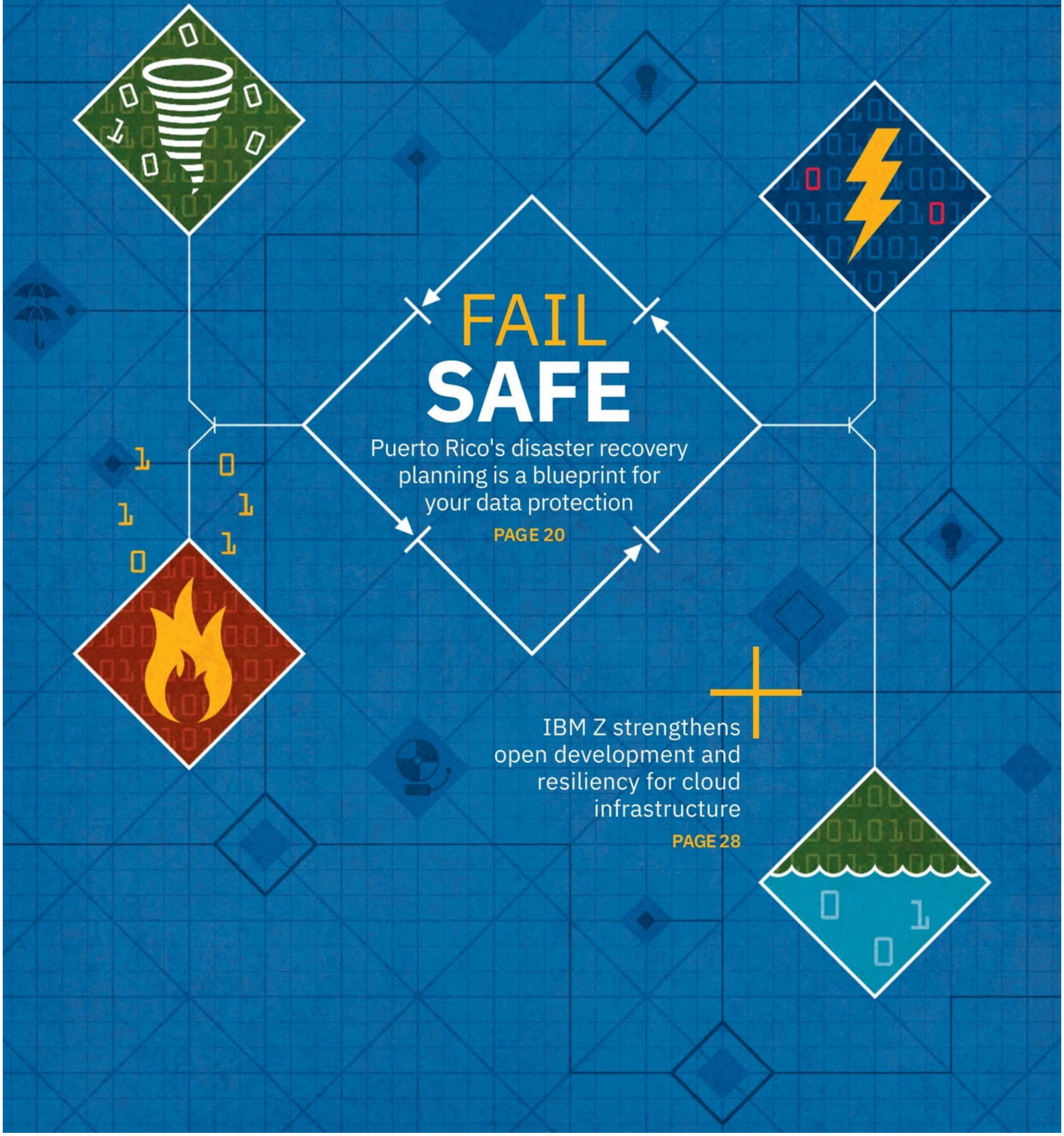
JULY/AUGUST 2019 IBMSYSTEMSMAG.COM

IBM Systems

IBM Z



FAIL SAFE

Puerto Rico's disaster recovery planning is a blueprint for your data protection

PAGE 20

IBM Z strengthens open development and resiliency for cloud infrastructure

PAGE 28

FAIL SAFE

Puerto Rico's disaster recovery planning is a blueprint for your data protection

By Karen E Lewis // Illustration by Jude Buffum

A fail-safe, effective disaster recovery (DR) plan—one that's documented and tested regularly—is essential for limiting downtime, avoiding lost revenue, ensuring a speedy recovery and allowing an organization to restore services to clients quickly. A reliable DR plan is not only good for business, it's also good for those affected by downtime and disasters.

A Perfect Storm for Disruption

The Department of Treasury of Puerto Rico learned a lot about the vulnerability of its systems after two successive hurricanes. The treasury handles all financial, income and tax data for public services. If the treasury's systems go down, people can't pay taxes and ports can't release merchandise, preventing vital tax income from being collected.

Up until 2017, the treasury generated daily backups to rudimentary DR cartridges that were kept in internal and external vaults. However, the treasury lacked a plan to restore systems if an outage affected its main business-critical IBM Z* server.

Better Equipped for Future Disasters

To rectify the situation, the treasury partnered with Truenorth, PSR and IBM to implement a more comprehensive disaster management system based on IBM Z solutions. An IBM z14* server replaced the existing production server. Using IBM Global Mirror, the department now replicates data asynchronously to a second IBM z14 at a DR site operated by another of the treasury's main contractors, Evertec. The treasury also refreshed its storage environment with IBM DS8884 hybrid storage and IBM TS7760 tape systems.

Tested annually, the treasury's new DR system ensures 100% of its applications will be operational in an alternate data center with a recovery point objective (RPO) and recovery time objective (RTO) under 35 hours. And, with additional configuration and hardware, that recovery window can be reduced to a couple of hours or less. "Today, most of our application landscape is protected by IBM technology. With effective availability measures in place, it's a huge weight off of our minds at the treasury," says Raúl Cruz Franqui, CIO, Department of Treasury of Puerto Rico.

Any Unplanned Outage Is Expensive

There's no denying earthquakes, flooding and hurricanes knock out vital systems and services. However, in today's connected society, natural disasters aren't the only threats. "A lot of disaster events are caused by power outages, internal and external security breaches or cyberattacks, and of course, simple human error," says David Petersen, IBM Distinguished Engineer and chief architect for GDPS.

No matter the cause, outages are expensive:

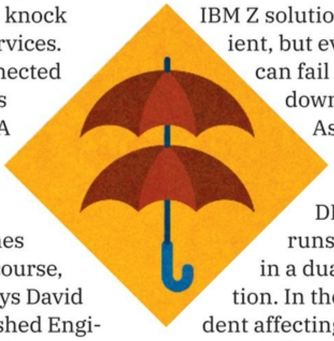
- The estimated cost of a cyberattack is $1.1 million, with the most impactful problems stemming from productivity loss and negative customer experience (bit.ly/2vbjvLX)
- The average cost of network downtime is $5,600 per minute (gtnr.it/2LWTvKU). For industries such as automotive assembly, downtime can cost as much as $22,000 per minute—that's $1.3 million per hour (bit.ly/2J5NwVQ).
- The average global cost of a data breach is $3.86 million (ibm.co/2O9kCHS)

The lost productivity, lost revenue, regulatory impact and reputation impact all add up. In an always-on world, dependence on technology is high and tolerance to disruption is low. When users encounter disruption, it doesn't take long before they jump on social media channels to express their dissatisfaction.

5 Ways to Keep Your Business on

How prepared is your team? Use these five best practices to help protect your systems and data from serious risk:

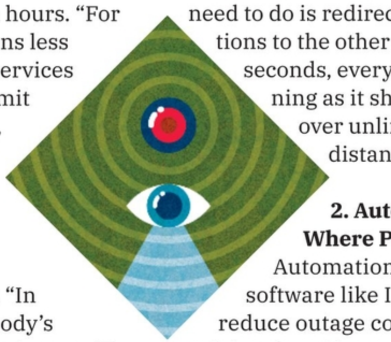
1. Redundancy Protection



IBM Z solutions are highly resilient, but even a mainframe can fail or need to be taken down for maintenance. As part of Department of Treasury of Puerto Rico's DR system, the team runs two IBM Z servers in a dual-site configuration. In the event of an incident affecting its primary data center, staff can switch over to the DR infrastructure (Evertec), resuming operations within hours. "For our citizens, this means less disruption to public services and the ability to submit their tax information, while the government can return to business-as-usual sooner," says Cruz Franqui.

In Petersen's view, "In a world where everybody's becoming more dependent on IT, there's an expectation that everything will always be available." IBM GDPS is a collection of offerings that can be tailored to meet the recovery objectives for your business. Each offering uses a combination of services, server and storage hardware/software-based replication and automation, and clustering software technologies to ensure that the solution satisfies your business objectives.

For example, GDPS Continuous Availability is ideally suited for clients needing the best possible availability (e.g., financial organizations). Using GDPS Continuous Availability, organizations can run multiple workloads where the active instances of the workloads are on either site (thereby making all sites active). Each server is then configured, so each active site is a standby site for the other. This approach gives you full utilization of your sites with the potential for continuous availability between them. If a problem occurs, all you need to do is redirect the connections to the other site, and within seconds, everything is running as it should be—even over unlimited global distances.



2. Automate Where Possible

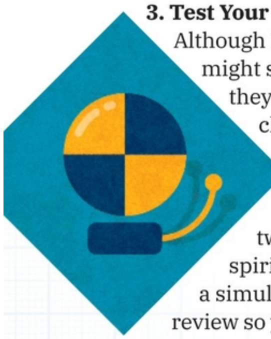
Automation or control software like IBM GDPS helps reduce outage costs by minimizing downtime and avoiding human error. If you have an incident, people are under stress and could make mistakes. Using control software, you can react immediately.

"Systems have gotten so reliable that when a problem does arise,

> *"In a world where everybody's becoming more dependent on IT, there's an expectation that everything will always be available."*
>
> *—David Petersen, IBM Distinguished Engineer and chief architect for GDPS*

people don't know how to recover from it," Petersen says. "By the time an administrator or operator has called the right people, precious time has slipped away. Using automation—where a system can monitor itself—can lead to faster recovery times."

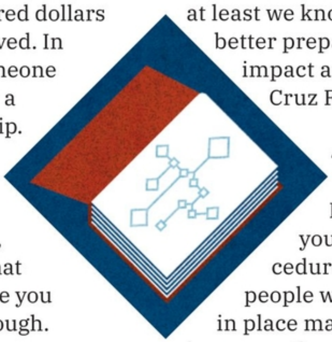
Take the scenario of credit cards, authorizations and fraud. If a card is stolen or compromised, it's going to be used within the first few hours. If your credit card provider is down for an hour, transactions within a couple hundred dollars are going to be approved. In another example, someone might be applying for a loan at a car dealership. That loan application might be sent to multiple banks. If your bank is offline, then you could lose that loan potential because you can't respond fast enough.



3. Test Your System

Although DR fire drills might sound stressful, they can help control chaos. As a best practice, a DR process should be tested at least twice a year. In the spirit of Agile, after a simulation, conduct a review so you can continue to improve.

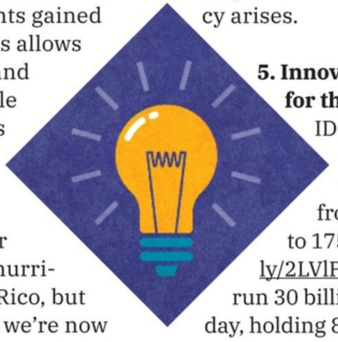
The IBM solution at the Department of Treasury of Puerto Rico enables the team to periodically simulate an outage of the main site and test failover to the alternate location. Using insights gained during these test runs allows the team to identify and fix any problems while isolating applications and data to ensure the entire environment is replicated accurately. "We never know when another hurricane may hit Puerto Rico, but at least we know that we're now better prepared to absorb the impact and recover quickly," Cruz Franqui notes.



4. Document Processes

Best practice dictates you document DR procedures thoroughly. The people who put your DR plan in place may not be around any longer, or they may not be available. Effective knowledge transfer helps everyone understand the environment, safeguarding the recovery process. "We are creating documentation that ensures that we know how to manage the solution long term and can communicate this information to new employees," says Cruz Franqui.

In another example, when the World Trade Center collapsed, although many companies had their DR sites off Manhattan in New Jersey, they couldn't get to them because all of the tunnels and bridges were closed. Having documentation in order will keep things on track when an emergency arises.



5. Innovate for the Future

IDC projects that worldwide digital data will grow from 33 ZB in 2018 to 175 ZB in 2025 (bit.ly/2LVlP5h). Mainframes run 30 billion transactions per day, holding 80% of the world's business data, and handle 90% of all credit transactions (bit.ly/2PJqaq6). More data to manage means more data to recover. By exploring capabilities designed to enhance, rather than complicate a DR plan, your approach will withstand emergencies, and grow with the needs of the organization.

New capabilities from leading-edge IBM Z solutions help ensure that the treasury can deliver vital services reliably and collect the necessary revenue to fund the government's operations. In the future, the treasury is looking to take advantage of new features like pervasive encryption to protect sensitive data, while reducing risk and simplifying compliance with IRS directives for encryption. Other advances being explored include using new blockchain capabilities to collect and distribute payments. This future strategy will help fortify the treasury's defense against cyberattacks and ransomware.

Peace of Mind

Achieving business continuity involves a trade-off between the cost of an outage or data loss with the investment required for achieving RPO and RTO. IBM solutions address each of these metrics. Robust, reliable and resilient IBM Z solutions are available to help you weather almost any storm.

> *"We never know when another hurricane may hit Puerto Rico, but at least we know that we're now better prepared to absorb the impact and recover quickly."*
>
> *—Raúl Cruz Franqui, CIO, Department of Treasury of Puerto Rico*