PREVENTING DOWNTIME THROUGH OPERATIONAL RESILIENCY.

SUNGARD® Availability Services

TODAY'S MOST COMMON CAUSES OF DOWNTIME AND HOW TO MINIMIZE THEIR IMPACT

Thought Leadership

WHITE PAPER

EXECUTIVE OVERVIEW

Organizations rely on IT to support their business. As they embrace global, 24/7 operations, their IT systems need to be right there with them, available at all times.

Operational risks are growing. The number of catastrophic disasters has increased dramatically over the last 15 years. At the same time, IT architectures are more distributed and complex as organizations adopt hybrid IT solutions that incorporate legacy systems, managed systems, virtualized systems, as well as the public and private cloud. Increasing complexity means that more can go wrong that can take IT systems down. And these types of outages can have a great impact on the organization.

To keep IT systems "always-on" in the face of increased disasters and operational risks, organizations must adopt a new paradigm of operational resilience. Rather than following a traditional disaster recovery approach of waiting until disaster strikes and then recovering systems after the fact, resilience focuses on proactively keeping IT systems running. This white paper describes the most common sources of IT downtime today and the key elements of an operational resilience program that can prevent IT downtime and eliminate business disruptions.

ROBUST RESILIENCY AND RECOVERY — MORE IMPORTANT THAN EVER

As organizations increasingly operate globally, serving customers in multiple time zones, and employees extend their workday and work on-the-go using mobile devices, today's organizations must operate 24/7. With IT at the center of these operations, enabling or touching upon virtually every aspect of business, continuous IT availability is more important than ever.

Failure to keep IT systems up and running can lead to considerable financial costs. According to a survey of organizations of various sizes by the Aberdeen Group[1], each hour of downtime sets the average respondent back $163,674.13 — with actual losses varying from $8,580.00 for small companies to as much as $686,250.00 for the largest companies. Organizations incur additional expenses when customers lose confidence in the company and switch to a competitor, employees can't perform their jobs, and IT staff must spend time resolving problems and recovering systems.

1 Aberdeen Group "Business Continuity and Disaster Recovery: Don't Go it Alone," June 2013–11–05.

THE KEY CAUSES OF DOWNTIME

Yet even as "always on" operations become more critical, risks to IT systems are increasing. Not only are traditional risks, such as natural and man-made disasters, becoming more frequent, increasing IT complexity means more common causes of outages, such as power failures and human error, can have more of an impact on operations.

CATASTROPHIC EVENTS

When most organizations think of the causes of downtime, the first thing they think of are catastrophic events. The number of catastrophic events and their financial consequences have been growing due to climate change.[2] Through the 80s and 90s, a typical year had two or three events with losses that totaled more than $1 billion and few years saw five or more such events. Losses usually added up to less than $20 million each year.

Since 1996, billion dollar events have become twice as frequent as in the preceding 15 years. And the dollar amount of losses keeps mounting. In 2012, the U.S. experienced 11 billion-dollar-plus-loss events with losses totaling more than $119 billion. A partial list of these events includes:

- Hurricane Sandy killed 131 people and caused losses estimated at $62 billion in the Northeast United States
- Yearlong drought and extreme heat that lead to at least 123 deaths and more than $35 billion in losses primarily due to crop failures across more than half the United States, from California north to Idaho and the Dakotas and east to Indiana and Illinois
- Hurricane Isaac over Louisiana and the Gulf that cost 9 dead and losses of $2 billion
- Tornados and severe thunderstorms in Texas, New Mexico and Colorado caused at least $3.75 billion in losses

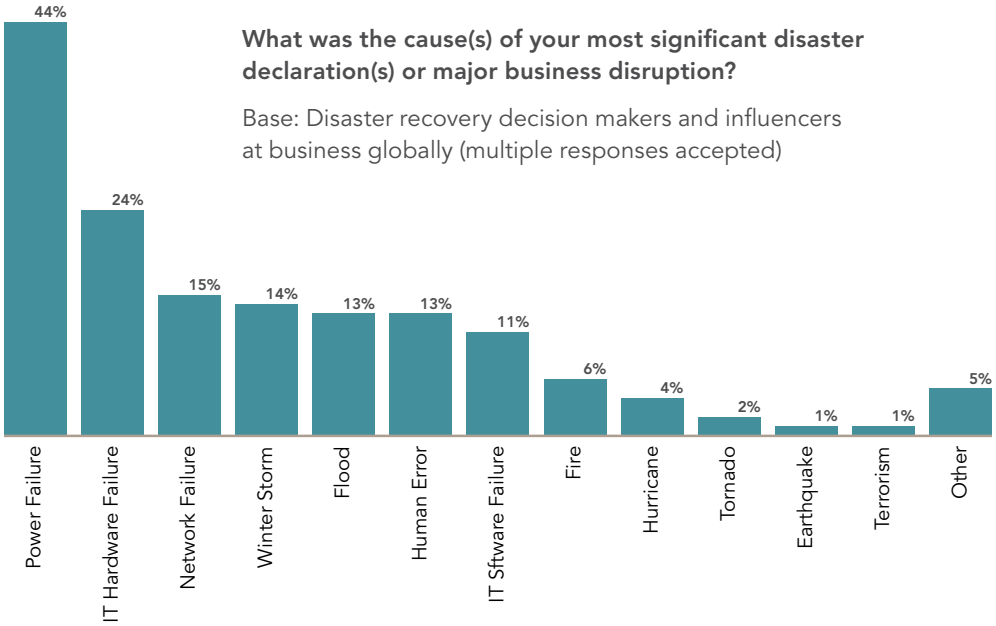
The previous year, 2011, was also a bad year for natural disasters with 14 events with losses over $1 billion; however, the total dollar amount was half that of 2012. When looked at in the overall context, 2011 and 2012 look not like anomalies but continuations of a frightening trend.

2 Earth Journal, "Losses to catastrophic weather events rank 2012 among the worst on record," by Ron Meador, 01/03/12.

In 2012, the U.S. experienced 11 billion-dollar-plus-loss events with losses totaling more than $119 billion.

MUNDANE CAUSES OF DOWNTIME

While catastrophic events are top-of-mind, the events that actually cause the most significant business disruptions are power, hardware, and network failures, as shown in the chart below. These events will have an increasing impact due to the complexity of today's systems. With the availability of ever-more powerful servers over the last decade and the widespread use of virtualization, a half dozen to a dozen critical applications might run on a single server. A problem with this server will impact multiple applications. This makes it all the more essential to reduce the chance of downtime and quickly recover from any problems.



Source: Forrester Research, "Five Steps to Improve Business Technology Resiliency Processes," Rachel Dines, October 24, 2013

HYBRID IT ENVIRONMENTS

Hybrid environments make maintaining uninterrupted business operations even more complex. Naturally, these systems face all the same risks of power, hardware or network failures as any other IT system. In addition, these environments have many interdependencies that need to be properly reflected in the recovery environment or organizations will be unable to recover the system within the required recovery point objective/recovery time objective (RPO/RTO)—if at all.

Consider the following situation. An organization hosts its Oracle ERP on servers in its in-house environment. The Oracle ERP includes a Human Resources module that stores information about employees and their access rights. Oracle feeds this data to an Active Directory server, which also runs in the organization's own environment. A cloud-based customer relationship management (CRM), in turn, uses this Active Directory to verify that an end user is still an employee before permitting him or her to log in.

The IT staff might think they don't have to worry about recovery for the CRM because this application is in the cloud and presumably protected by the service provider. However, if they fail to make recovery for Active Directory a high enough priority and Active Directory goes down, the sales reps will be unable to access the CRM even though it resides in the cloud because the system won't have access to their permissions.

As a result, it's critical for organizations to understand the interdependencies and to make recovery plans accordingly or they'll be unable to meet their RPO/RTOs.

CLOUD ENVIRONMENTS

Many SMBs are moving applications and functionality to the cloud. Cloud computing can create a false sense of security should a disaster strike because the cloud service provider is responsible for ensuring availability. Yet, cloud applications can still have interdependencies with functionality and systems that aren't in the cloud, as described in the previous section. SMBs need to be aware of these interdependencies and design their recovery plans accordingly.

WHAT'S NEXT?

Even as organizations continue to grow ever more reliant on IT, all of these causes of downtime will only continue to grow worse. Analysts and industry experts predict:

1 IT ENVIRONMENTS WILL CONTINUE TO BECOME MORE COMPLEX — AND SO WILL THEIR RECOVERY.

2 NATURAL DISASTERS WILL ONLY INCREASE DUE TO CLIMATE CHANGE.

WHAT'S NEEDED? OPERATIONAL RESILIENCE

To keep up with the increasing risks while maintaining IT system uptime, organizations need to move away from thinking in terms of recovery and adopt the paradigm of operational resilience. Recovery assumes that systems must first suffer an outage before they can resume normal operations. It implies extended periods of downtime with potential data loss. In contrast, resilience is about ensuring that the business can absorb the impact of any unexpected occurrence without disrupting business operations.

Business technology resilience has the following characteristics; it:

- Focuses on continuous availability
- Limits downtime as much as possible through preventative measures and rapid response
- Drives investments by the need to reduce the cost of downtime and stay competitive
- Matches recovery objectives to business requirements
- Looks to measure downtime in minutes to hours
- Focuses on all likely sources of business disruption
- Emphasizes continuous management and improvement, testing, and preparedness

RESILIENCE: A HOLISTIC DISCIPLINE

To achieve resilience, organizations need to shift the focus of their IT operations. Disaster recovery is about performing disciplines such as security, business continuity, disaster recovery and IT service management. In contrast, resilience focuses on applying best practices to orchestrate these individual disciplines into a coordinated whole that spans all layers and functions in the organization and helps ensure that the organization's overall mission is achieved.

Resilience requires that organizations enhance existing skills while approaching production and recovery environments in a new way. Rather than simply knowing how to implement technology, resilience requires people with a different type of experience and mindset. These people need to understand the big picture and be able to:

- Map out the business and mission critical processes and the importance of each to the business.
- Figure out what applications support these processes and their interdependencies.
- Appraise the cost of downtime for each mission-critical and business-critical process. This often requires converting technical challenges and bottlenecks into operational processes that are financially quantifiable. For example, when a server goes down, a certain department is affected, which costs the company "X" dollars.
- Evaluate how quickly each process needs to be restored.
- Determine how much data the organization can afford to lose for each critical process.
- Estimate potential threats.
- Assess what mitigating technologies could be used to reduce the downtime risk or downtime duration.
- Define, draft and validate a plan leveraging those technologies and integrating them into the daily culture of the organization.
- Test the plan on an ongoing basis.

Implementing a resilience plan is thus not just about technology, it also incorporates people and processes. It requires change management and people skills to help the organization operate the plan properly. For example, rather than just implementing backup, a resilience program would include developing a backup plan, communicating with employees about the importance of backup, training them on the new system, and testing to ensure it works correctly and that people are using it properly.

SUNGARD SOLUTIONS DELIVER OPERATIONAL RESILIENCE

With the complexity and new skillsets required to implement an operational resilience program, many organizations may find themselves without the necessary capabilities in house. SunGard Recovery Services provide a comprehensive and affordable suite of recovery services that cover organizations' needs for complex data and application protection and recovery for everything from mainframes to virtual machines. Our solutions bridge the gap between traditional recovery and cloud-based recovery for customers' enterprise IT infrastructure, providing a single plan for all their recovery requirements. SunGard Recovery Services allow organizations to define their level of operational resiliency, supporting a full spectrum of RTOs starting at 10 minutes. For example, an organization might want to bring up its ERP right away while another application can wait a few hours. With a specialty in managing complex hybrid infrastructures, we advise organizations on how to set up their RPO/RTO objectives to mitigate the recovery risks of application interdependencies across a heterogeneous production environment.

SUNGARD® Availability Services

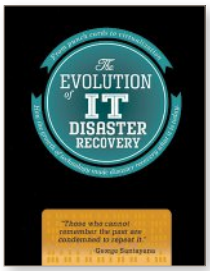
TODAY'S MOST COMMON CAUSES OF DOWNTIME AND HOW TO MINIMIZE THEIR IMPACT

Thought Leadership

CONCLUSION

To keep up with the growing operational risks caused by natural disasters and increasing IT complexity, organizations are turning to the new paradigm of operational resilience. This model requires not just technology, but also new ways of thinking and new processes. SunGard Recovery Services provide the expertise and experience to design, develop, support and maintain customers' operational resilience programs, providing a full range of services to maintain operations for organizations with complex hybrid infrastructures.

ADDITIONAL READING



The Evolution of IT Disaster Recovery Infographic

Ten Things to Look for in a Disaster Recovery Provider Checklist

FOR ADDITIONAL INFORMATION

For more information please visit our website at: www.sungardas.com/disaster-recovery

Connect with Us

About SunGard Availability Services

SunGard Availability Services provides disaster recovery services, managed IT services, information availability consulting services and business continuity management software. To learn more, visit www.sungardas.com or call 1-888-270-3657.