PROTECTED
HARBOR

# THE 7 STEPS TO PREVENT IT-CAUSED OUTAGES

A Comprehensive Approach

2023

# TABLE OF CONTENTS

## Introduction

## Incident Review

## Incident Review

# Introduction

In today's technology-driven world, businesses heavily rely on their IT infrastructure, making the potential impact of outages significant and far-reaching. Statistics reveal the alarming effects of IT-caused outages on businesses worldwide. According to a recent study by Business Wire, IT outages cost companies an estimated $700 billion annually, with an average outage duration of four hours.

Additionally, our research suggests that 90% of organizations have experienced at least one IT outage in the past two years, emphasizing the widespread nature of this problem. These figures underscore the critical need for organizations to implement proactive measures to prevent IT-caused outages.

To address this pressing issue, we present a comprehensive approach comprising seven crucial steps to prevent IT-caused outages. These steps encompass a range of preventive measures that organizations can adopt, from enhancing infrastructure redundancy to implementing robust monitoring and incident response protocols. Organizations can significantly minimize the likelihood and impact of IT-caused outages by implementing these steps.

"Within the realm of technology, we can learn valuable lessons from two major incidents that shook the world. One happened in November '21 when Google Cloud experienced an outage; the other occurred in October '21, affecting Facebook, Instagram, WhatsApp, and related services. These incidents showed us the vulnerabilities and weaknesses in our systems.

By studying them, we can take proactive steps to prevent future outages. Instead of focusing on the chaos they caused, let's use them as guides to make our systems more robust and resilient. Doing so can create a future where outages are just minor blips in our journey towards progress."

"In the realm of technology, where innovation dances with possibility, occasional outages serve as a humbling reminder that even the mightiest systems are crafted by human hands. Embrace these temporary setbacks as catalysts for growth, for they fortify our resolve to construct a future where seamless connectivity reigns supreme."

**Richard Luna**
**CEO of Protected Harbor**

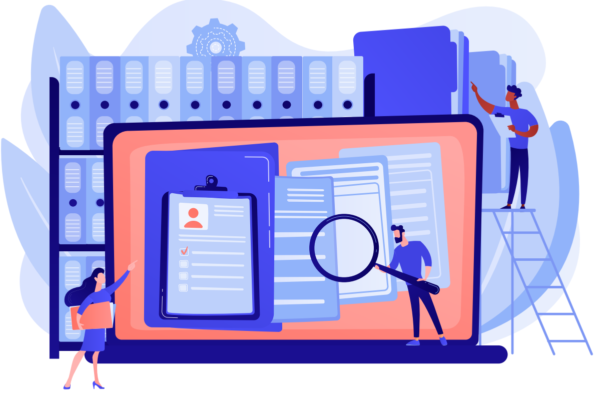
Organizations require a comprehensive and proactive support system to fortify their IT infrastructure and prevent outages. The whitepaper concludes with an overview of the Protected Harbor Managed Services Program.

This program offers a holistic approach to IT infrastructure management, combining expert guidance, continuous monitoring, and rapid incident response. By leveraging the capabilities of Protected Harbor, organizations can maintain a resilient IT environment and prevent costly outages.

Let's explore the seven key steps essential for preventing IT-caused outages. These steps serve as proactive measures to ensure the stability and reliability of IT systems. Once we have a solid understanding of these preventative measures, we will delve into the specifics of two incidents, providing valuable lessons learned from each case.

## Step 1- Establish a Comprehensive Asset Inventory

In the first step of preventing IT-caused outages, it is crucial to establish a comprehensive asset inventory. This entails identifying, documenting, and tracking all IT assets within an organization. Let's explore the importance of asset management and how it can be implemented effectively.



### • Importance of Asset Management

Effective asset management is essential for maintaining a stable IT environment. By clearly understanding all IT assets, organizations can proactively address potential vulnerabilities, plan for upgrades or replacements, and ensure compliance with regulatory requirements. Asset management also helps optimize resource allocation and budgeting, resulting in cost savings and improved operational efficiency.

### • Identification and Documentation of IT Assets

The first aspect of establishing an asset inventory is identifying and documenting all IT assets across the organization. This includes hardware devices, such as servers, routers, and workstations, as well as software applications and licenses. Conducting a thorough inventory assessment, considering physical and virtual assets, is crucial to ensure everything is noticed.

For example, asset management software can be utilized in a large enterprise to scan the network and automatically collect information about connected devices. This software can provide detailed reports on hardware specifications, installed software, and license information, facilitating documentation.

### • Tracking and Regular Updates

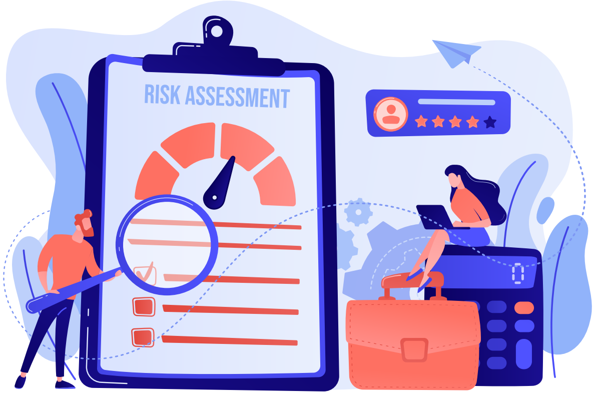
Once the initial asset inventory is established, it is essential to implement a system for tracking and regular updates. IT assets are dynamic and can change over time due to hardware replacements, software upgrades, or new acquisitions. Therefore, maintaining an up-to-date asset inventory is crucial for effectively managing and mitigating potential risks.

Organizations can employ asset management tools that enable real-time tracking of assets and automate the update process. For instance, a cloud-based asset management system can provide a centralized repository for asset information,allowing authorized personnel to access and update asset details from anywhere, anytime.

A practical application of comprehensive asset inventory management can be seen in a financial institution. The institution can ensure compliance with regulatory standards and streamline the audit process by accurately tracking all IT assets, including servers, network devices, and software licenses. Additionally, it enables proactive monitoring and maintenance, reducing the risk of unexpected outages and optimizing resource allocation.

## Step 2- Conduct Regular Risk Assessments

Conducting regular risk assessments is crucial in the second step of preventing IT-caused outages. This involves identifying vulnerabilities and potential risks within an organization's IT infrastructure. Let's explore the importance of risk assessments and how they can be implemented effectively.



### • Understanding Vulnerabilities and Risks

To effectively prevent outages, organizations must comprehensively understand their IT infrastructure's vulnerabilities and associated risks. This includes identifying potential security threats, system weaknesses, and external factors that could impact operations. By conducting regular risk assessments, organizations can proactively identify and address potential issues before they escalate into outages.

For example, in the healthcare industry, a risk assessment might involve identifying vulnerabilities in electronic health record (EHR) systems, such as outdated software versions or inadequate access controls. Healthcare organizations can implement appropriate security measures to protect patient data and prevent system failures by understanding these vulnerabilities.

### • Prioritizing Critical Systems and Processes

Not all IT systems and processes have the same criticality level for an organization's operations. Prioritizing and focusing on critical systems and processes during risk assessments is essential. By doing so, organizations can allocate resources and efforts effectively to mitigate risks with the highest potential impact on their operations.
For instance, a risk assessment might prioritize core banking systems that handle customer transactions and account management in the banking sector. Identifying vulnerabilities in these critical systems allows banks to prioritize security updates, conduct regular penetration testing, and implement robust disaster recovery measures to prevent disruptions to essential banking services.

### • Mitigating Risks through Effective Controls

The final step in conducting risk assessments is to develop and implement adequate controls to mitigate identified risks. This involves putting security measures, protocols, and monitoring mechanisms in place to prevent or minimize potential outages' impact.

Real-life applications of risk mitigation controls can be seen in the aviation industry. Airlines conduct regular risk assessments to identify potential vulnerabilities in their flight operations systems. To mitigate these risks, they implement redundant systems, backup power supplies, and continuous monitoring tools to ensure the reliability and safety of their operations, minimizing the chances of flight delays or cancellations due to IT failures.
Organizations can proactively identify and mitigate potential risks by conducting regular risk assessments and implementing effective controls, minimizing the likelihood of IT-caused outages. Risk assessments provide valuable insights into vulnerabilities and threats, enabling organizations to prioritize critical systems, allocate resources effectively, and implement appropriate security measures. These proactive measures strengthen an organization's IT infrastructure, enhance resilience, and ensure continuous operations despite potential risks and threats.

## Step 3- Implement Robust Change Management Processes

Implementing robust change management processes is a crucial step in preventing IT-related outages. Change management ensures that any changes made to IT systems, configurations, or software are carefully planned, tested, and implemented without causing disruptions to the normal functioning of the systems. Here's how it works in real-life situations:

First, organizations establish clear rules and steps for making changes. These rules help guide requesting, evaluating, approving, and implementing changes. It's like having a set of instructions to follow.

Second, thorough testing is done before making any changes. This is like checking if something works appropriately before you use it. Testing in a controlled environment can identify and fix any problems or issues before the changes are made live.

Finally, changes are implemented in a way that minimizes any impact on the regular functioning of the systems. This means choosing the right time to make the changes, such as when there is less activity, and having backup plans in case something goes wrong. Communication with the people affected by the changes is essential to manage their expectations.

For example, in the software industry, companies have transparent processes to manage updates and releases. They carefully assess and test changes to ensure they don't introduce bugs or compatibility issues that could cause system failures. In the telecommunications sector, changes to network infrastructure are tested in simulation environments to ensure they don't disrupt communication services. Similarly, in e-commerce, website changes are scheduled and tested during off-peak hours to avoid disruptions during busy shopping periods.

Organizations can reduce the risk of IT-related outages by following robust change management processes. These processes provide a structured approach to handling changes, ensuring that modifications are implemented smoothly and without causing disruptions to the systems.

## Step 4- Enhance Monitoring and Alerting Systems

Enhancing monitoring and alerting systems is a critical step in preventing IT-caused outages. By closely monitoring the performance of IT systems and proactively detecting issues, organizations can take timely actions to avoid potential failures. Let's explore how this step is applied in real-life situations:

First, organizations implement real-time performance monitoring. This involves continuously tracking the performance metrics of IT systems, such as response times, resource utilization, and network traffic. By monitoring these metrics in real time, organizations can identify any abnormalities or bottlenecks that may indicate a potential outage. For example, temperature sensors are used in a data center to monitor the cooling system and ensure that it operates within optimal ranges to prevent overheating and equipment failures.

Second, proactive alerting mechanisms are put in place. These mechanisms automatically generate alerts or notifications when predefined thresholds or conditions are met. This helps IT teams stay informed about potential issues and take immediate actions to prevent them from escalating. For instance, if the bandwidth usage exceeds a certain threshold in network infrastructure, an alert is triggered, prompting IT administrators to investigate and address the issue promptly.

Third, organizations utilize automated monitoring tools. These tools leverage artificial intelligence and machine learning algorithms to analyze vast data and identify patterns or anomalies. By using these tools, IT teams can detect potential issues that may go unnoticed by manual monitoring alone. For example, automated monitoring tools in a cloud computing environment can analyze system logs and detect unusual access patterns that may indicate a security breach.

Real-life applications of enhanced monitoring and alerting systems across various industries. In the financial sector, banks utilize real-time monitoring to track transaction processing times and detect any delays or errors that may impact customer transactions.

In the healthcare industry, hospitals employ monitoring systems to continuously monitor critical medical devices and patient data, ensuring timely interventions and preventing disruptions in patient care. Similarly, e-commerce platforms utilize automated monitoring tools to track website performance, identify performance bottlenecks, and address them promptly to provide a seamless online shopping experience.

Organizations can proactively identify and address potential issues by implementing robust monitoring and alerting systems before they escalate into outages. These systems enable IT teams to stay informed, take prompt actions, and ensure the uninterrupted functioning of critical IT systems.

## Step 5- Strengthen IT Infrastructure and Redundancy

To prevent IT-caused outages, it is crucial to have a strong and resilient IT infrastructure. Infrastructure strengthening involves assessing and upgrading hardware and software components, implementing redundant systems and network architecture, and ensuring scalability and flexibility. Let's explore these steps with real-life applications and examples:

### • Assessing and Upgrading Hardware and Software

Organizations need to assess and upgrade their hardware and software regularly. This includes evaluating the performance and capacity of servers, storage devices, networking equipment, and other infrastructure components.

Upgrading outdated or inadequate hardware and software helps prevent performance bottlenecks and potential failures. For instance, a company experiencing slow website load times may upgrade its servers and optimize its database to handle increased user traffic efficiently.

### • Implementing Redundant Systems and Network Architecture

Implementing redundant systems and network architecture is essential. Redundancy involves having backup systems or components that can take over in case of a failure. This redundancy can be achieved through redundant servers, network links, power supplies, or data backups. For example, data centers often have redundant power sources, such as uninterruptible power supplies (UPS) and backup generators, to ensure continuous power supply in case of a power outage.

### • Ensuring Scalability and Flexibility

Organizations should ensure scalability and flexibility in their IT infrastructure. Scalability allows the infrastructure to handle increased demands or sudden spikes in user activity without causing disruptions. This can be achieved through technologies like cloud computing, which can scale resources up or down as needed. For instance, an e-commerce website that experiences high traffic during seasonal sales events can scale its infrastructure resources to handle the increased workload efficiently.

By strengthening the IT infrastructure and implementing redundancy, organizations can minimize the risk of outages caused by hardware or software failures, network issues, or unexpected surges in demand. These measures enhance the IT systems' reliability, performance, and resilience, ensuring business continuity and customer satisfaction.

## Step 6- Foster a Culture of Continuous Learning and Improvement

To prevent IT outages, it is crucial to cultivate a culture where learning and improvement are at the forefront. This involves implementing training and skill development programs to enhance the knowledge and capabilities of your IT team. They can stay updated with the latest technologies and best practices by providing the necessary resources and opportunities to expand their skills.

Conducting incident post-mortems and root cause analysis is crucial. When an outage or failure occurs, it is essential to investigate and understand the underlying reasons. This process helps identify any gaps or weaknesses in your systems or processes, allowing you to make improvements and prevent similar incidents in the future.

For example, if a software bug caused an outage, the post-mortem analysis can highlight the need for better testing protocols or code review practices.

Encouraging collaboration and knowledge sharing among team members is another vital aspect. By creating an environment where individuals can freely exchange ideas and insights, you harness the collective wisdom of your team. Real-life scenarios, such as organizing regular knowledge-sharing sessions or establishing internal forums for discussion, can facilitate sharing lessons learned, best practices, and innovative ideas.

An example of fostering a continuous learning and improvement culture is implementing a regular training program for IT staff on emerging security threats. This ensures they have the necessary skills and knowledge to identify and mitigate potential risks. Additionally, conducting incident post-mortems after a significant outage helps identify areas for improvement, such as enhancing backup systems or implementing better monitoring tools.

By prioritizing continuous learning and improvement, you empower your IT team to proactively address challenges, adapt to changes, and optimize your IT infrastructure to minimize the risk of outages and ensure smooth operations.

## Step 7- Develop and Test Comprehensive Disaster Recovery Plans

To safeguard against IT outages, it is crucial to have well-defined and regularly tested disaster recovery plans in place. This involves creating robust strategies to handle potential disruptions and minimize their impact on your business operations.

Firstly, it is essential to develop comprehensive disaster recovery strategies that outline the steps and procedures to be followed during an outage or disaster. This includes identifying critical systems and data, determining recovery time (RTOs) and recovery point objectives (RPOs), and establishing backup and restoration processes. Real-life examples of disaster recovery strategies include setting up off-site data backups, implementing redundant systems, and leveraging cloud-based disaster recovery services.

Regular testing and simulation exercises are vital to ensure the effectiveness of your disaster recovery plans. By simulating different outage scenarios and testing the recovery procedures, you can identify gaps or weaknesses in your strategies and make necessary improvements.

This testing can involve conducting mock drills, simulating system failures, or even performing full-scale recovery exercises. Real-life application of this step includes performing periodic disaster recovery tests to validate the recovery process and ensure that all critical systems and personnel are prepared for any potential disruptions.

Documenting and updating your recovery plans is also crucial. As your IT infrastructure evolves and new technologies emerge, keeping your disaster recovery plans up to date is essential. This involves documenting all recovery procedures, including contact information, system configurations, and step-by-step instructions.

Additionally, regularly reviewing and updating these plans is vital to reflect any changes in your IT environment or business processes. Real-life scenarios for documentation and updates can include maintaining an accessible and centralized repository for recovery plans, assigning responsible individuals for plan maintenance, and conducting periodic reviews to incorporate lessons learned from previous incidents.

By developing and regularly testing comprehensive disaster recovery plans, you can minimize downtime, protect critical data, and ensure a swift and effective response to IT outages or disasters. This step is crucial for maintaining business continuity and minimizing potential disruptions' financial and reputational impact.

# INCIDENT REVIEW: GOOGLE CLOUD OUTAGE, NOVEMBER 2021

In November 2021, Google Cloud experienced a significant outage that impacted numerous websites and services. The incident resulted in widespread disruption for end users and highlighted the complexity of managing and resolving such technical issues.

During the outage, users attempting to access various websites encountered a 404 error page associated with the Google bot. This unexpected behavior caused confusion and frustration among users, who attempted to reload pages and tried different URL variations, resulting in the same error.

From a technical standpoint, there were initial speculations about the cause of the outage. Some users considered potential issues with Google's Public DNS or a new feature implementation that redirected non-resolvable domains to Google's IP. However, these theories were quickly ruled out as the root cause.

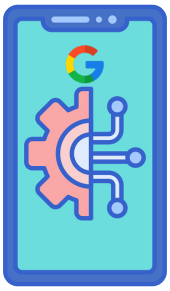
To investigate the situation further, affected users turned to several other platforms, namely other monitoring and testing service. Through this platform, it became evident that multiple websites were experiencing the same error message, and all were Google Cloud customers. This indicated that the problem lay within Google's cloud infrastructure.

Despite users seeking information on Google's status page, no updates were initially posted. It took approximately thirty minutes from the start of the issues for any information to be provided on the status page.

This incident highlights the complexity and impact of outages on users and the importance of timely communication and resolution. It also emphasizes the need for robust incident response strategies and effective communication channels to minimize user disruptions during such technical incidents.

The Google Cloud outage in November 2021 had varying impacts on different Google Cloud services, resulting in customer disruptions and issues across multiple regions. Here are some additional details regarding the specific services affected:

**1. Google App Engine:** Experienced a significant decrease in traffic by approximately 80% in central parts of the U.S. and Western Europe. This decrease in traffic impacted the availability and accessibility of applications hosted on Google App Engine.



**2. Google Cloud Networking:** Customers of Google Cloud Networking needed help making changes to website load balancing. This led to the appearance of 404 error pages when users tried to access affected websites.

**3. Google Cloud Functions:** Users utilizing Google Cloud Functions faced disruptions and potential unavailability during the outage. Google Cloud Functions is a serverless computing service offered by Google Cloud.

**4. Google Cloud Run:** Customers using Google Cloud Run, which allows for the deployment and scaling of containers, experienced issues, and potential service interruptions.

**5. Google App Engine Flex:** Similar to Google App Engine, Google App Engine Flex, which provides a flexible and scalable platform for running applications, was impacted, leading to service disruptions.

**6. Apigee:** Apigee, an API management platform provided by Google Cloud, was affected during the outage. This likely impacted the functionality and availability of APIs utilizing the Apigee platform.

**7. Firebase:** Customers using Firebase, a mobile and web development platform, also experienced disruptions and service issues due to the Google Cloud outage.
The breadth of services impacted during the incident underscores the widespread nature of the outage and its impact on various Google Cloud customers relying on these services for their applications, networking, APIs, and other functionalities.

Google Cloud issued an apology for the service outage and acknowledged the inconvenience it caused its customers. The root cause of the incident, as stated on the organization's status page, was attributed to "a latent bug in a network configuration service that was triggered during a leader election charge." To prevent similar issues in the future, Google Cloud has implemented two safeguards for enhanced protection.

This recent outage, amidst a year of similar incidents, highlights the significant impact a public cloud vendor outage can have downstream. It also emphasizes the vulnerability of enterprises to third-party vendor outages. Many businesses heavily rely on the public Internet, services, and infrastructure to operate and deliver digital experiences to their clients. While there are advantages to this reliance, the challenge lies in the fact that these organizations need more control over the underlying infrastructure that supports their operations.

GOOGLE Responds to Incident

## Three key lessons learned from the google cloud outage that can be applied to your own business:

### Lesson 1: Communicate clearly with end users through proper error pages.

- Don't assume users will find your status page or rely on social media for updates.
- Create a custom error page that reflects your brand, apologizes for the failure, and provides clear messaging.
- Make the error page engaging and relatable to end users to maintain a positive impression.

### Lesson 2: Implement comprehensive observability outside your environment.

- Use an IPM (Infrastructure Performance Monitoring) approach to monitor services outside your cloud or data center.
- Don't solely rely on code tracing and logs; have a broader view of your services.
- Proactively observe your services and the infrastructure providers you rely on to identify issues before they impact your users.

### Lesson 3: Track service-level agreements (SLAs) and mean time to resolution (MTTR).

- Monitor the performance of your teams and providers in resolving issues.
- Build trust by holding them accountable and verifying their actions.
- Utilize real-time data from independent monitoring and observability solutions to accurately track the impact of issues and understand their duration.

By applying these lessons, you can enhance communication with users, ensure proactive monitoring, and track the effectiveness of issue resolution, thereby improving the reliability and trustworthiness of your services.

# INCIDENT REVIEW: FACEBOOK OUTAGE, OCTOBER 2021

The popular social media platforms Facebook, Instagram, WhatsApp, Messenger, and Oculus VR faced an unprecedented situation on Monday, October 4th, when they all went down simultaneously for a significant duration. The outage began before 16:00 UTC and lasted until approximately 21:05 UTC, causing inconvenience to users worldwide.

Users trying to access these platforms encountered error messages during this period instead. However, things gradually started returning to normal after 21:05 UTC.

The incident sparked discussions on social media about the significance of these platforms in our lives. It raised questions about the potential risks of relying heavily on a single technological platform that can experience global failures.

In simpler terms, it was an unusual event where popular social networks like Facebook, Instagram, WhatsApp, Messenger, and Oculus VR stopped working worldwide for several hours. This outage made people realize how much we depend on these platforms and the risks involved when such a dominant technology experiences widespread issues.

> "We know how much people and businesses depend on us to stay connected daily. We recognize the impact that outages, like the one experienced today, have on people's lives, and we take our responsibility seriously in keeping everyone informed about service disruptions. We apologize to all those affected, and our team is actively investigating the incident to understand better what occurred. Our goal is to strengthen our infrastructure to enhance its resilience continuously."

**Facebook Responds to Incident**

Santosh Janardhan, VP, Infrastructure, Facebook

## During the occurrence of 503 errors, specific HTTP headers were observed. These headers included information such as the HTTP/2 503 response code, indicating a service unavailable status.

- Access-control-allow-origin: The access-control-allow-origin header allowed requests from any origin.
- Content-length: 2959 The content-length header indicated the size of the response content, which was 2959 bytes.
- Content-type: text/html; and charset=utf-8 - The content-type header specified that the content was in HTML format with a character encoding of UTF-8.
- Date: Mon, 04 Oct 2021 16:48:36 GMT - The date header indicated the timestamp of the response.
- Proxy-status: no_server_available - The proxy-status header indicated that no server was available to handle the request then.

These headers provided insights into the nature and details of the 503 errors experienced.

### Lesson Learned from the Facebook Outage: Transparency and Recovery

In a recent analysis, the Facebook team provided valuable insights into the cause of the outage on October 5, 2021. Contrary to initial speculations, the incident did not result from DNS or BGP issues. Instead, it stemmed from a routine maintenance task performed by Facebook staff. This task was intended to assess the availability of their global backbone network.
Unfortunately, this routine job had unintended consequences, disrupting their backbone connections. As a result, Facebook routers could not communicate with their data centers. The BGP routes to their DNS servers were withdrawn from the network to ensure safety.

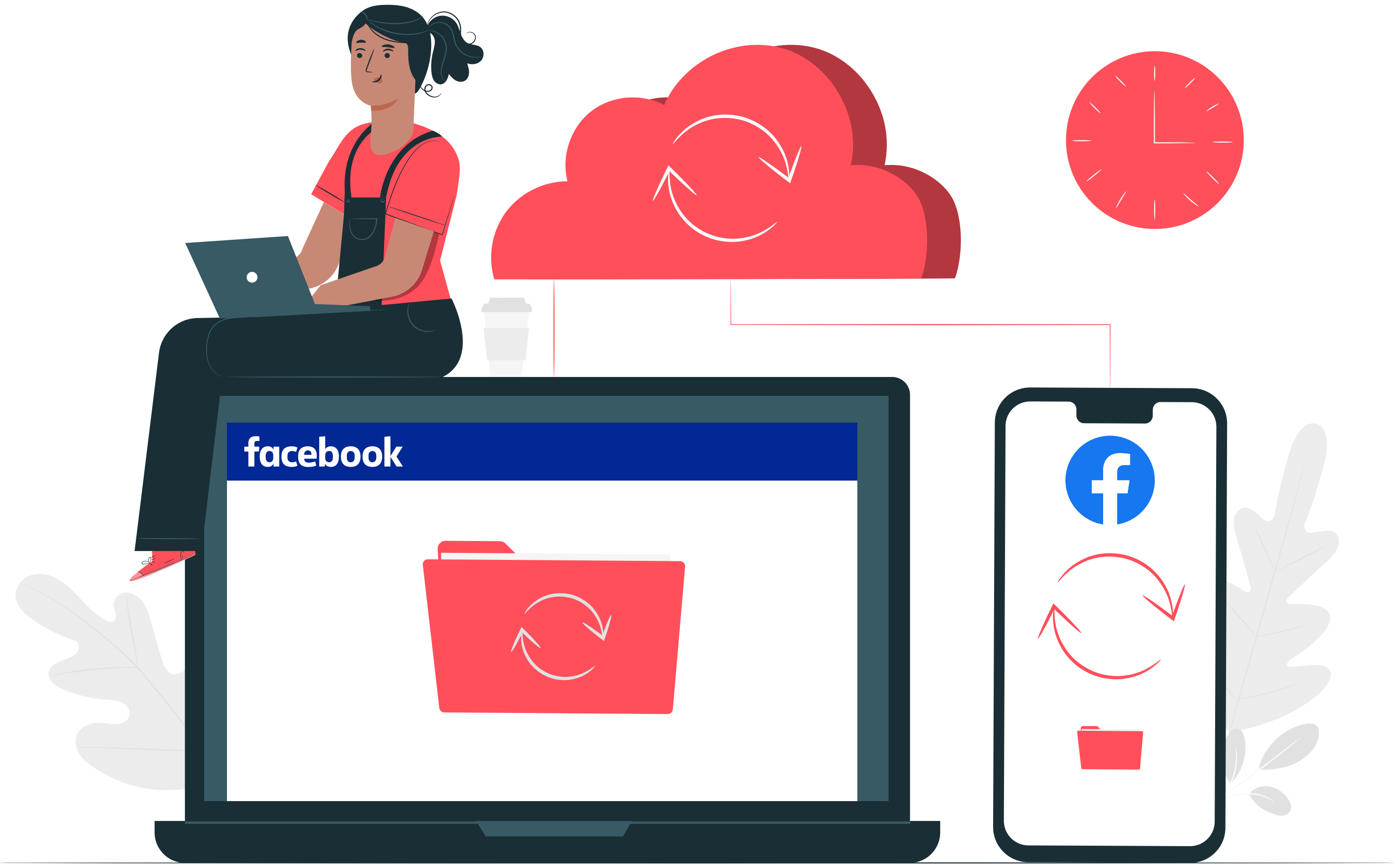
It is worth appreciating the Facebook team for their swift recovery efforts and, most notably, their transparency in sharing the details of the incident. This incident serves as a reminder of the importance of open communication and taking responsibility for technological failures.

The speed of detecting and addressing an outage is crucial. It is important to have well-defined runbooks or procedures to guide the response during such incidents. It is also necessary to ensure that your systems are designed in a way that prevents dependencies. For example, the systems employees use to fix issues should rely on something other than the same infrastructure they are trying to fix.

In situations like these, troubleshooting can be complex. In the case of Facebook, the initial symptoms were related to HTTP and DNS errors, which eventually affected the Border Gateway Protocol (BGP).

In simpler terms, it is vital to identify and resolve outages quickly. Having clear instructions (runbooks) for handling such situations is essential. Additionally, it is crucial to design systems to prevent dependencies, such as ensuring that the tools used for fixing issues are not reliant on the same infrastructure that needs fixing.

Troubleshooting during these incidents is often more complex. In the case of Facebook, the problems initially appeared as errors related to web and network services, but they eventually impacted the routing protocol used for directing internet traffic (BGP).



# PROTECTED HARBOR MANAGED SERVICES PROGRAM

Unleash the Power of Round-the-Clock Support with Protected Harbor

Experience the peace of mind that comes with 24/7/365 support from our seasoned team of experts. With Protected Harbor, you can rely on our dedicated professionals to provide comprehensive training, seamless onboarding assistance, and invaluable best practices tailored to your organization's needs.

Our team seamlessly integrates with yours, offering regular KPI updates and identifying optimization opportunities to ensure your organization achieves unrivaled Internet Resilience. With our world-class expertise and an additional layer of protection, you can confidently navigate the digital landscape.

-Discover the full range of services and benefits at-
https://www.protectedharbor.com/protected-full-service"

**Need Faster Systems?**
Choose Protected Harbor Full Service

**Need Cybersecurity?**
Choose Protected Harbor Cybersecurity Services

**No More Outages?**
Choose Protected Harbor Full Service

**Need Support Year Round?**
Choose Protected Harbor Managed Services Program

"By partnering with us, you can confidently navigate the complex IT landscape, knowing that we are dedicated to preventing and mitigating IT outages. Together, we will build resilient infrastructure and proactively address vulnerabilities, ensuring uninterrupted business operations. Trust us to be your strategic ally in the journey towards a robust and outage-free IT environment."

RICHARD LUNA
CEO of Protected Harbor

# CONCLUSION

IT outages can happen unexpectedly and have significant consequences for businesses. In today's digital landscape, where reliance on cloud services and the internet is high, it's crucial to be prepared for downtime or performance issues. Whether the problem arises from technical faults, misconfigurations, cloud providers, or internet service providers, understanding the source of the issue and how to respond is essential to minimize damage.

Deep visibility into your IT infrastructure and digital experience is vital to address IT outages effectively. With a Performance Monitoring platform explicitly designed for Managed IT Services, you can proactively identify and resolve issues promptly while improving your future response.

As you develop your IT and Internet Resilience strategy, ensure that your visibility perspective covers all critical areas. This includes monitoring internal networks, cloud providers, workforce productivity, BGP routing, and global CDN traffic optimization. By gathering comprehensive data, you can swiftly respond to issues, communicate effectively with your customers, and hold your service providers accountable for meeting their SLAs. You can seek compensation, switch providers, or enhance failover options if necessary.

IT Outage Preparedness is no longer just an option; it has become a business imperative for Managed IT Services in 2023. By embracing a proactive approach and leveraging the proper monitoring tools, you can minimize the impact of IT outages and ensure uninterrupted operations for your clients.

Taking a holistic approach to IT-caused outage prevention brings numerous advantages. It minimizes the financial costs and reputational damage associated with downtime and increases productivity, customer satisfaction, and overall business resilience. By proactively addressing potential risks and continuously improving your IT infrastructure and processes, you can position your business for long-term success in the digital era.

Since 2009, we've been a trusted software engineering partner for top brands, offering innovative solutions. We're a boutique digital transformation consultancy and software development company based in New York, serving clients nationwide.

We believe in customized approaches, not one-size-fits-all solutions. We begin by assessing your current technology and identifying areas for improvement. Then, we create a tailored IT service plan to help you achieve your business goals quickly and cost-effectively. Our data center solutions optimize your critical business applications' infrastructure.

Our commitment goes beyond solving problems. We provide 24/7/365 customer service, ensuring a live person can assist you whenever you need us. We aim to connect on a human level, becoming an extension of your team. With a 98% client retention rate, we prioritize building long-term partnerships.

As technology evolves, we stay ahead to offer more value, options, and flexibility. Our constantly changing products and services keep pace with the changing world, giving you access to tools to propel your business forward.

Choose us as your Managed Services partner and experience unparalleled support, innovation, and customer service. Let's embark on a transformative journey, realizing your digital goals.

www.protectedharbor.com