

In a world that depends on technology, outages and downtime can have significant effects on revenue, service levels, and customer satisfaction. Proactive planning can help organizations reduce downtime and foster resilience.

Building Resilient IT Operations: Proactive Strategies to Minimize Downtime and Enhance Business Continuity

November 2024

Written by: Snow Tempest, Research Manager, IT Service Management

Introduction: More Threats to Continuity Lead to More Value in Resilience

Organizations face a rapidly evolving landscape of challenges, including cybersecurity threats, geopolitical instability, and the growing complexity of technology systems. These factors drive organizations to develop adaptive, resilient infrastructures that can withstand and respond to various pressures. In this environment, proactive planning and resilience are no longer optional but essential.

Operational failures come with a hefty price tag. A major incident can cost an organization millions in lost revenue, productivity, and reputation damage. Resilient infrastructure is critical to avoiding these costs and ensuring business continuity.

In addition, technology has become more complex than ever as new solutions integrate into environments that contain aging systems. To foster innovation, organizations must continue to add and update technologies; however, these changes bring risks. By acknowledging the potential for incidents and downtime, organizations can gain a competitive advantage by proactively addressing problems before they arise.

Definitions

- » **Incident:** An unplanned interruption to a service or reduction in the quality of a service
- » **Problem:** A cause or potential cause of one or more incidents

AT A GLANCE

KEY TAKEAWAY

Organizations sometimes experience downtime or other incidents due to factors over which they don't have complete control. What they can control is how they respond. With a plan for incident response, modern tooling, and a culture of learning, organizations can react more quickly when problems occur — or even prevent them from happening in the first place.

The Reality: Technology Breaks — It's About the Response

Preparedness and the ability to reduce downtime provide significant benefits for organizations and their clients. Reducing downtime reduces costs, prevents revenue loss, and ensures compliance with service level agreements (SLAs). Fewer incidents and outages help employees feel supported, enhancing engagement and retention. Customers also benefit from increased engagement when interacting with employees or accessing services through technology. Overall, organizations gain a competitive advantage from these benefits, along with improved uptime and faster issue resolution.

Achieving these benefits involves planning, tooling, and human oversight. Organizations should develop plans to handle incidents, including processes for diagnosing, addressing, communicating, and resolving issues, as well as notifying the teams involved. Proper tools can help predict and prevent incidents and assist in resolutions. Even with tools in place, organizations should maintain some human oversight due to the high stakes of incidents.

Organizations must prepare for the "new normal" of technology as the world's dependence upon it grows. Technology must perform reliably and be secure from growing cybersecurity threats. It also must cope with geopolitical instability, which can lead to unreliable infrastructure and other stability threats.

Planning and Preparedness

Given that incidents are certain to arise, organizations should create a plan to address them when they occur. Modernizing technology operations enables better incident detection from the outset. Modern IT operations tools offer monitoring and event correlation to identify incidents before users notice and report them. For instance, AIOps tools can correlate alerts to facilitate the identification of more widespread issues. In IDC's October 2023 *AIOps and Observability Survey*, respondents ranked the top 3 most important AIOps capabilities as: root cause analysis; proactive, predictive performance and trend analysis; and automated incident response workflows. This survey response indicates that effective incident identification can enable automated resolution steps, including diagnostics, troubleshooting, and self-healing. Components of a comprehensive plan include:

- » **Incident management:** Although there is an automatic resolution for many incidents, human intervention remains necessary at times. Organizations should have practices and tools in place for effective incident management, alerting, and prioritization. Understanding the business context of technology aids in triage by enabling responders to see which business systems a particular incident affects. Effective alerting also involves understanding the business context and previous incident response history to quickly identify relevant stakeholders. Once the right people engage, incident management tools can help them get up to speed by providing context for alerts and a summary of any prior work.
- » **Automated tools:** After incident alerting is in place, the next step is to develop streamlined, intelligent incident management processes. Artificial intelligence (AI) and machine learning (ML) can help human responders by suggesting remediation steps and providing embedded intelligence features, such as generating summaries of the status. In addition, automating common remediation steps enhances overall incident management efficiency. Advanced AI features may also suggest further automation. Insight into the business context of technology helps determine how to communicate with affected individuals.

- » **Communication strategies:** The incident management process should include communication planning. For internal communication, organizations should coordinate a response that minimizes distractions for the team addressing the incident while updating internal stakeholders about the issue and its progress. For external communications, coordinating with customer service operations benefits IT teams by helping them understand if there have been customer reports and whether to reclassify the incident severity according to its impact on customers.
- » **Learning from incidents:** Organizations can practice continuous improvement by establishing procedures to learn from incidents. Practitioners can conduct post-incident reviews for major incidents, studying the response to adapt plans for future incident management. In addition, understanding the root cause of an incident reveals ways to prevent similar issues or resolve them faster in the future, potentially through automation.

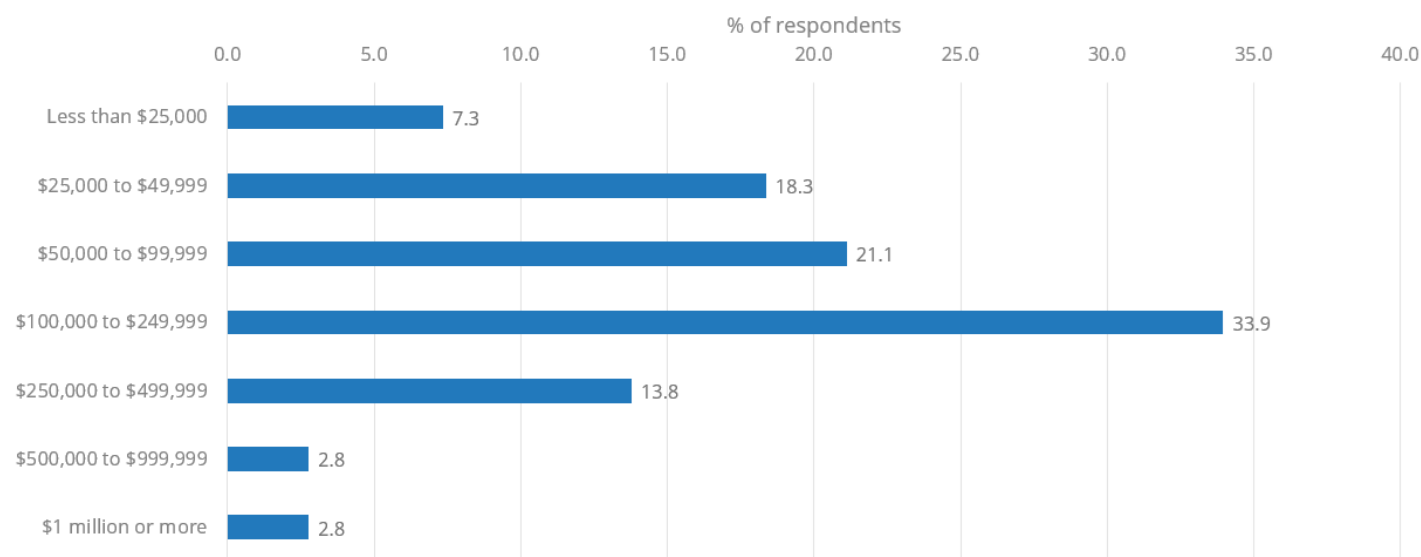
This learning practice can also help anticipate future incidents, providing opportunities to address them before end users notice. By learning from past issues, practitioners can identify where to best implement predictive technology, alerts, and automations. Previous insights can inform the creation of playbooks for guided remediation.

The Cost of Downtime: Financial and Reputational Effects

Downtime can have various costs for an organization. An IDC survey found that respondents from larger enterprises estimated the cost of a single hour of downtime for a revenue-generating service at \$100,000 to \$249,999 (see Figure 1). Organizations may also face costs from fines for violating SLAs or regulatory noncompliance. Beyond revenue loss, costs include damage to relationships with affected customers and reputational harm. A plan to prevent incidents and address them quickly, along with effective communication, can strengthen organizational resilience.

FIGURE 1: *Cost of an Hour of Downtime*

Q What's the average cost of an hour of downtime/outage when a revenue-generating production service is impacted?



n = 109

Source: IDC's AIOPs and Observability Survey, November 2022

Considerations: Balancing Modernization and Risk

Organizations need to balance risk. They must modernize and update their systems and processes while considering the downsides of change. There are also risks in not changing, such as technical debt and security vulnerabilities. In addition, development teams often face pressure to deliver high-impact features quickly, which can lead to significant issues if deployments encounter problems. Having plans to manage the impacts of change can help. As organizations modernize, they should focus on improving their incident and problem management practices and their IT operations, drawing from their experiences. As previously indicated, outages and downtime will occur occasionally due to these factors, so organizations should have communication and customer support plans in place.

Trends: Managing More Technology

Trends likely to increase the need for planning for incidents and outages include the continuing rise of digital business and the push for greater use of automation and AI. Both trends pressure organizations to implement technology changes and make the business more dependent on technology.

Conclusion: Planning for Resilience

As organizations push toward digital operations, they become increasingly dependent on technology to maintain business continuity. This reliance means that outages and downtime have more significant effects on revenue, service levels, and customer satisfaction. In this environment, improved operational resilience can provide an additional competitive advantage alongside the benefits of technology updates.

Improved operational resilience can add an additional competitive advantage by mitigating risks from technology updates.

About the Analyst



Snow Tempest, Research Manager, IT Service Management

Snow Tempest is research manager for IDC's IT Service Management Program, responsible for delivering research and advisory for IT executives, vendor management teams, and investment executives. Snow's research coverage includes IT service management, software asset management, and the use of AI and NLP for service management.

MESSAGE FROM THE SPONSOR

PagerDuty Operations Cloud

The PagerDuty Operations Cloud is the platform for mission-critical, time-critical operations work in the modern enterprise. Through the power of AI and automation, it detects and diagnoses disruptive events, mobilizes the right team members to respond, and streamlines infrastructure and workflows across your digital operations. The Operations Cloud is essential infrastructure for revolutionizing digital operations to compete and win as a modern digital business. Learn more at: <https://www.pagerduty.com/platform/operations-cloud/>



The content in this paper was adapted from existing IDC research published on www.idc.com.

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2024 IDC. Reproduction without written permission is completely forbidden.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
blogs.idc.com
www.idc.com