IT Outages:
No room for outages in a customer-centric world

Customers have little tolerance for outages: businesses must do better with unified IT OPS

Customer service is the glue that binds organizations and end-users together. Whether in a B2B or B2C context, customer experience is the foundation on which competitive advantage and growth can be built. Increasingly, in today's digital-centric world, this means paying close attention to your IT infrastructure: the servers, networks, storage and clouds that power crucial customer-facing applications and services.

Unfortunately, this is where organizations are still failing. IT outages remain a key impediment to customer loyalty and long-term value, yet many businesses view them simply as a cost of doing business. Instead, they need to prioritize the customer experience by investing in unified IT operations and monitoring to optimize performance and service delivery.

Sprawling IT systems

In many organizations, even the best-intentioned plans to improve visibility into and control over IT operations can be hampered by existing infrastructure, processes and culture. Despite the emphasis on digital transformation, many firms operate sprawling IT systems which are continuously being patched up. Disparate, decentralized systems don't talk to each other, meaning IT is fed a patchwork of operational information. For IT teams who need answers quickly, this is a recipe for disaster. And to make things worse, many of these systems are outside the control of IT, adding an extra layer of opacity and complexity.

Digital transformation may be all the rage in the boardroom, but frequently IT is not included at the top table. Too often it's viewed as an afterthought instead of a strategic necessity – a cost center rather than a value driver. Consequently, investments in apps and services are not matched by improvements in performance monitoring, leading to inevitable outages down the line.

The siloed nature of IT does not help its cause. The lack of communication between departments prevents sharing of insights and best practice. In many cases, duplicate technologies are installed, leading to tool sprawl which perpetuates the cycle. Each team is destined to carry on as its predecessors did, fighting fires and auto-renewing superfluous tools, which in turn undermines their ability to optimize customer service. Gartner claims that by 2020, 80% of IT operations tools and processes in IoT projects will be unable to meet business requirements. Until IT is viewed in a more strategic way, it's hard to see this changing.

To err is human

These challenges become more pronounced when one considers the problems humans can cause in an organization. Everybody makes mistakes. In fact, according to Gartner, "the undisputed number one cause of network outages is human error." However, it's how you react to, plan for and work to mitigate these problems that matters.

Consider the maintenance contractor who happened to pull out the wrong cable at a key British Airways datacenter, triggering a system reboot and consequential shut-down. That resulted in a financial hit of £80m to the airline. Similar outages at TSB, Verizon, Delta and many other big-name brands show just how common IT outages have become.

Human error is one thing, but an even more common issue is humans missing potential IT issues because they don't have the time to inspect the problem properly in the first place. This can lead to cascading faults, with one error triggering another, sometimes imperilling entire IT systems.

> ❝ The undisputed number one cause of network outages is human error. ❞
>
> GARTNER

A single pane of glass

The only way to tackle these challenges is to gain a single version of the truth across your entire IT ecosystem and consolidate all disparate technologies. This can only be achieved by securing visibility across all areas of IT, unifying it via a centralized monitoring system. At its heart, IT monitoring carried out effectively is a key component of IT Operations Management which, is designed to "manage the provisioning, capacity, performance and availability of the computing, networking and application environment" (Gartner), and not only provides a holistic view of the health of the system, but also provides a single version of the truth by preventing tool sprawl. This avoids the duplication of effort and unites siloed teams. Often when companies do decide to consolidate systems, they also take the opportunity to upgrade or re-architect their existing solutions, thereby taking advantage

of the most modern implementation strategies, architectures and versions. Being able to capably monitor this – which is often done in a way that has not been done before – is essential to ensure success, and the single pane of glass approach is not only the most efficient, but effective too.

With enhanced insight derived from IT monitoring, organizations can detect, assess and fix any problems early on, across the entire IT stack. For example, a disk failure is not an issue which will bring a business to its knees. It will slow processes down, but it won't cause the sort of issues associated with major IT outages. However, it is exactly the sort of problem which can easily cascade for businesses, so enabling automatic remediation at source can be a great help in reducing outage risk.

Combine IT monitoring with a high degree of automation and you're well on the way to minimizing the impact of human error and issues being missed. Automation in particular helps to drive consistency and reduce the need for manual configurations, which is where problems can otherwise creep in.

These benefits also extend to audit trails. By providing a clear, automated timeline of what happened and when, businesses can pinpoint issues and improve accountability at scale. Ultimately, this will also help to improve the user experience by ensuring problems are always dealt with promptly.

Time for change

It may be tough to make these changes overnight. In many organizations, they'll be predicated on cultural change, which is needed so that business leaders start to treat IT with the strategic importance it deserves, and allow CIOs greater decision-making autonomy. However, it's vitally important they do start to move in this direction.

With greater visibility, driven through monitoring and centralized IT Operations, organizations can be more confident in adopting best practices such as running regular threat and vulnerability assessments, conducting configuration reviews and including operation process validation checkpoints. With these, they can reduce IT bottlenecks, nip problems in the bud to minimize the chance of major outages and, ultimately, drive closer bonds of trust with customers.

Modern consumers are a fickle bunch and it's never been easier for them to switch brands. Don't give them an excuse to - put the right tools in place to stop unnecessary outages.

🖐 **FIND OUT MORE**

✉ **sales@opsview.com**

📞 **USA: +1 866 662 4160**

📞 **EMEA: +44 1183 242 100**