WEATHERING THE STORM

Zero In On Downtime For Long-Term Business Continuity and Customer Satisfaction



Small business has changed dramatically within the last decade. No change has been more profound than our dependency on information technology (IT) systems to support critical day-to-day business functions.

In today's increasingly competitive high-tech environment, it is critical that all business operations run smoothly and efficiently. Business momentum, employee productivity and customer service all depend on an IT infrastructure that must be both accessible and secure at all times. Constant network availability has become essential to most small and midsize businesses (SMBs) today.

This reliance on IT systems has also created a stronger link between data center accessibility and total cost of ownership (TCO). Even minimal amounts of unplanned downtime today will result in lost revenue, productivity and negatively impact overall brand reputation.

Preventing or rebounding from downtime was once deemed the IT team's problem, however, this unprecedented modern-day dependence on technology has made the frequency and costs of downtime more of a business problem. Prolonged or recurring downtime can cripple small businesses and requires the attention and understanding of C-suite management in order to be properly addressed.

Unfortunately, many executives at SMBs are still not as tuned into daily network operations as they need to be. For this reason, they lack a true awareness of the frequency of downtime. This lack of insight and visibility is regrettably putting far too many SMB sat an increased risk for downtime and the costs associated with it.

WEATHERING THE STORM



It is imperative that all levels at a SMB have insight into the probability and implications of downtime. This is the only way to maximize uptime and the availability of essential IT applications without over inflating the total cost of ownership of data center infrastructure.

Bridging the Gap Between C-Suite Executives and In-House IT Teams

While most C-level executives are well aware that network operations play a pivotal role in productivity, service and profitability, they don't have the same awareness as IT personnel when it comes to the frequency of downtime and what makes their data center infrastructure vulnerable to it. Worse yet, many SMBs don't even have in-house IT staff – meaning nobody in the company or organization has any insight into the problem.

At the same time, even when internal IT personnel is on deck, many support technicians fail to recognize the financial implications of downtime when it comes to lost revenue, lost productivity and lost customers.



Calculate the True Cost of Downtime

According to the *Aberdeen Group*, a business intelligence research firm, downtime is costing companies 65% more per hour these days than just two years ago. 2012 data calculated downtime costs at the $165,000 mark compared to the $100,000 of 2010.

WEATHERING THE STORM

According to *Symantec's 2011 SMB Disaster Preparedness Survey*, small businesses lose an average of $3,000 each day from downed systems and networks. Medium sized businesses bleed even more money, losing an average of $23,000 each day.

C-Suite management at SMBs must consider both the direct and indirect costs of downtime. Direct costs are:

- Wasted wages paid to idle employees
- Sales lost during the outages
- The expensive emergency service/ repair bill issued by the on-call IT technician brought in to get your business back up and running.

Indirect costs, such as lost customers who have moved on after one too many "Our server is down" messages, are more difficult to quantify but more costly – equating to roughly 62% of all network downtime costs. A specific dollar amount cannot be placed on lost productivity, the long-term consequences of damaged reputation and wasted opportunities that accompany each downtime event.

This is why Chief Information Officers (CIOs) and IT support alike don't have the visibility or insight to understand what the average downtime event truly costs them. The residual effects of a network outage are typically much more costly than costs related to identifying the root cause of the failure and repairing or replacing any physical hardware.

But so many C-level executives remain mindful of only what downtime costs them in terms of repair or replacement costs. They also tend to gloss over the fact that their day-to-day business processes are more susceptible to outages and inaccessible data than they think.

WEATHERING THE STORM



Zero In On Infrastructure Vulnerability to Data Center Downtime

Leading Causes of Downtime

Power Outages – 48%

Accidental Data Deletion – 31%

Employee Created – 29%

Virus/Malware – 25%

Application Failure – 20%

Power Related Outages – Vulnerabilities to a data center's power still rank as one of the leading causes of unplanned network outages and can often be catastrophic. Particularly costly are UPS (Uninterrupted Power Supply) related failures (this includes batteries) and generator failures.

ZERO IN

To minimize the impact that power outages have on data center operations, and to prevent a potentially catastrophic unavailability of the data center, a dependable backup system is needed. This ensures the backup of critical data and applications is always in place in the event of equipment failure.

The integration of comprehensive infrastructure monitoring and management tools also minimizes the costs associated with identifying and repairing power system failures.

Accidental Data Deletion and Employee Created Downtime–

Simple human error is a prevalent cause of downtime. Whether months of data is unintentionally lost in a backup error, a power cord is unplugged, a busy IT technician overlooks routine maintenance and alert monitoring, or there is an error in judgment during an emergency, to err is human and apparently quite frequent as well.

WEATHERING THE STORM

A study by the Gartner Group, an IT research and advisory firm, projected that through 2015, 80% of downtime will be due to people and process issues.

In the fall of 2010, foursquare – a widely used mobile check-in app – had a highly publicized outage of eleven hours, followed by another shorter service disruption the next day. All three million users of the app were affected and it was a chain of human mistakes that led to both outages. IT techs noticed that a server was storing too much data, but as the support team tried to resolve the issue, all the servers went down.

ZERO IN

Regardless of proper training, or the quality of IT technician hires, human mistakes will likely always lead to instances of a downed data center or network, especially considering the expected learning curve of adapting to new technologies.

Ensuring proper communication amongst team members and adequate training at all levels is critical. Of course, it goes without saying that having a comprehensive backup strategy is also a necessity to counteract downtime and ensure business continuity regardless of who is having a bad day.

Virus/Malware/Hacks – SMBs are often guilty of thinking they are immune to hackers, viruses and malware. According to a National Cyber Alliance and Symantec survey, 77% of SMBs don't believe they're at risk for cybercrime while 83% admit to having no formal measures in place to counter these threats. This isn'tmerely a threat to your data; it puts your bank account and the sensitive data of your customers at risk.

ZERO IN

Passwords should be regularly changed every few months. They should also be strong. This means no more passwords like "password" or "1234567." Employees must be educated on security and precautionary measures. And there is no excuse for not having data backed up in this era of cloud computing and virtualization - where the entire contents of physical server – including the operating system, applications, patches and all data - can easily and cost-effectively be grouped

into one software bundle or virtual server.

Application Failure – Many applications or their components contribute to recurring downtime. While virtualization offers many multi-faceted advantages it has also further exacerbated overlapping applications in the infrastructure. One small application component failure is now likely to impact many applications.

ZERO IN

It is critical that all components are profiled and there is a general understanding as to what each application does – the hardware resources used by the application and the software it integrates with. Identifying an owner will allow for better monitoring and recognition of failure points.



Conclusion

Despite the risks of downtime, many SMBs still don't feel they're at any real risk. There is an overall sentiment of "It won't happen to me." It can be assumed that many hear the word "disaster" and mistakenly assess the immediate risk of natural disasters, such as hurricanes or earthquakes, impacting their day-to-day business. While those events, along with floods and fires, definitely contribute to a large number of unplanned prolonged outages, the truth is there is a new breed of modern era "disaster" culprits that can very literally happen on any given day. Downed networks and data centers from power outages, human error, viruses and malware, and application failure are much more probable and could be just as fatal to SMBs.

WEATHERING THE STORM

C-suite executives at SMBs must honestly assess their risk, quantify downtime costs, and improve disaster recovery efforts. In terms of ROI (Return on Investment) of business technology, it's important to remember that conventional disaster recovery can be expensive since it requires more time and resources. Stored data on backup tapes can also be more prone to error. Additionally, off-site backup tapes will always lead to prolonged downtime since recovery hinges on the retrieval and delivery of these tapes to the data center.

Many smaller and medium sized businesses are turning to new technology trends like virtualization and cloud computing as a cost effective means to better prepare for outages and the loss of critical business information. According to *Symantec's 2012 Disaster Preparedness Survey,* 26% of SMB executives cited disaster preparedness as a moderate to large influencer on their choice to move to a virtualized server infrastructure, 30% said minimizing downtime influenced their decision to move to public clouds, and 32% said a quicker recovery time affected their decision to move a private cloud.

SMBs can benefit from a little help when it comes to properly implementing and leveraging this new technology to strengthen their disaster recovery efforts. Access to a 24/7 NOC (Network Operations Center) team offering remote monitoring and management solutions, along with a 24/7 help desk, can help SMBs improve backup, monitoring and troubleshooting processes for maximum uptime and business continuity.

Contact us for more information
ht@sostechgroup.com
410-559-7020