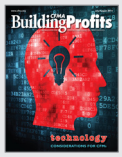

BY NATHAN WHITTACRE

HOW SMALL CONTRACTORS CAN
Protect Against Big Network Risks

About 55% of businesses claim to know how much it will cost if their systems go down; however, only 18% know the actual figure.[1]

Network downtime can happen at any moment and come in any form. Systems can go offline due to aging components, failing network connections, natural disasters, or human error. Such security issues as network intrusion or virus attacks can also threaten the integrity of your company's data.

It is important to acquire and maintain an effective IT environment that can adapt to your company's growing demands and changing needs. In many small and mid-size businesses, current IT systems may not be up-to-date or easy to manage, which sets the stage for potential problems down the road. Some critical components of an effective IT infrastructure include servers, storage devices, workstations, software, and connections coming into your office.

It is imperative to have these up and running at all times (with minimal scheduled downtime for repairs or upgrades) to maintain business momentum and employee productivity.

What's at Stake?

The main concern for most businesses that experience downtime is the potential loss of profits. The average small business stands to lose $12,500 per hour of complete downtime (i.e., when staff cannot work and customers cannot be served).[2] Multiply that by an eight-hour day and the result is a staggering $100,000 for a small business.

Companies that suffer from server downtime are subject to not only loss of sales and productivity, but also customer satisfaction. However, one of the most threatening ramifications of server downtime is loss of data; only 6% of businesses will survive after enduring server data loss.

The restoration process not only causes headaches and stress, but also lost wages paid to employees scheduled to work

during those days, unexpected purchase costs, and costs to build and restore server and customer satisfaction. Here is a breakdown of direct and indirect costs for a business experiencing downtime.

Direct/Tangible Costs	Indirect/Intangible Costs
Lost transaction revenue	Lost business opportunities
Lost wages	Loss of employees and/or employee morale
Lost inventory	Decrease in stock value
Remedial labor costs	Loss of customer/partner goodwill
Marketing costs	Brand damage
Bank fees	Driving business to competitors
Legal penalties from not delivering on Service Level Agreements (SLAs)	Bad publicity/press

The Solution: High Availability Systems

If a business cannot accept any downtime due to system failures, there are options to provide high availability. The two most popular ways to provide better resiliency against system failures are cloud computing and virtualization.

Cloud Computing

Many businesses are looking to cloud-based solutions to provide high availability. Cloud computing generally refers to moving software, service, or hardware from the company's internal server systems onto the Internet. Although some companies have what are known as "private clouds," cloud computing generally refers to another company managing, maintaining, or providing all the services for a specific computing function.

Cloud solutions can be a cost-effective way to offload system infrastructure expenses to a third party and move a capital expense to an operating expense. It can also reduce IT management requirements by outsourcing those functions to the companies that maintain the cloud services. Additionally, the cloud provider includes backup services, hardware redundancy, and higher levels of security in its systems than can be implemented in a small business.

However, there are disadvantages to moving systems to the cloud. Some considerations before moving are the financial stability of the cloud company, guaranteed availability (usually provided by SLAs), infrastructure security and data breach responsibilities, and data ownership. Consider consulting an IT professional before making the decision to move.

Virtualization

For companies that cannot move their systems to the cloud, the virtualization of their servers is highly recommended. In its basic sense, virtualization is the separation of the hardware and software of the computer.

Traditionally, computer hardware was purchased with a single preloaded operating system dedicated to one function (e.g., file servers, e-mail servers, SQL databases, or accounting systems). In the small business environment, these systems would run a Microsoft Server operating system. Most servers are built with redundant power supplies, redundant hard drives, and high-end hardware components, thus limiting hardware failures. The operating system was also more reliable than desktop systems, with better built-in security.

However, even with all these protections in place, there is still a chance of catastrophic failure. Virtualization allows for continuation of computing services in case of this type of failure by separating the hardware from the operating system and replicating the operating system (along with all the running software and data) across two or more physical servers. Additionally, multiple operating systems can work on one physical server, potentially reducing the overall capital expenses.

For example, a company running a Microsoft network with a domain controller, e-mail server, file server, and database server would traditionally have to purchase four individual physical servers. If one of those servers went down, then the functions provided by that server would be down until the problem could be fixed. With virtualization, the company may only need to purchase three physical servers. The different operating systems would be virtualized.

In this example, the domain controller and e-mail server could run on physical server number one, the file and database servers on physical server number two, and the third server could be a standby server. All the data would be replicated and shared between all three physical servers.

In this scenario, if the second physical server experienced a catastrophic failure, then the virtual servers running on it could start running immediately on the third physical server with limited or no downtime or data loss. The physical server that failed could be repaired or replaced without affecting business functions; once restored, system redundancy would be back online.

For additional protection, these systems could be replicated offsite in a remote office or data center. In the event of

catastrophic failure at the main location, all services could be moved to the offsite location with limited downtime.

While virtualization can add cost and complexity to IT infrastructure, the value that it brings to an organization can easily be quantified compared to the expense of downtime.

Business Impact Assessment: Steps & Best Practices

Some events like power station issues, hardware failure, network failure, or network intrusion may be within your control and can be prevented by having a plan in place. Other events like natural disasters or a backhoe operator who accidently severs power or network lines would be out of your control. According to research, 40% of downtime is related to power station issues, while 25% is the result of hardware failure, 19% is due to network failure, and 15% is the result of human error.[3]

Before you figure out a plan, the steps below can help determine what is acceptable downtime for your company and the impact it will have on the bottom line and staff productivity:

1) Identify critical business functions based on data/application integrity and time sensitivity to downtime.

2) Determine the maximum outage that a specific function can sustain before it impacts the business.

3) Determine the costs associated with the various disruption scenarios.

4) Identify the financial (revenue), productivity (expenses), and personal impact (goodwill) of a business function disruption.

5) Assess both long-term (permanent) and short-term outages or disruptions.

6) Determine the recovery priority of each function.

7) Identify the most critical or vital data and the resources required to resume a business function.

8) Define alternatives to sustain continuity.

9) Define the various solutions/tactics that can be used to reduce or eliminate the costs of a business function outage.

Train and encourage staff members to follow all of these steps. Now, let's look at best practices your company may want to implement.

Offsite & Automated Backups

It is very important to back up your company's data offsite every day through an automated system that delivers reports and confirmation that your data has been backed up. If you are only backing up your server, then make sure to train your employees to save all important files directly to the server (not their workstations).

Power Outage Backups

A power outage can literally "fry" your computer equipment, causing downtime and possible data loss if you don't have the previous step in place. Make sure to have your server and networking equipment connected to a battery backup unit that is powerful enough to sustain your server if the power goes out to allow enough time to close running programs and turn off the server.

Most battery backup units last for about three years, so as time goes by, the unit that could once power your server for one hour may eventually only power it for 20 minutes. Keep an inventory with purchase dates and replace these units as they age. When possible, install units into your workstations.

Quality High-Speed Internet Connection

Most businesses rely on Internet service for their everyday operations. When choosing a provider, make sure its services are reliable and that it offers a service level guarantee and scalable speeds so you can easily upgrade if needed. Good questions to ask when choosing a provider are:

- How much downtime did you experience in the past year?
- When you experience downtime, how long does it take you to bring the Internet connection back up?
- Do you have a download and upload speed guarantee?

True Redundant Failover Solution

In some cases, even the most reliable provider and Internet connection will have an outage. If your company cannot afford more than a few minutes of downtime, it is highly recommended to set up a backup Internet connection with a failover solution. In this solution, another provider installs Internet in your building and sets up an Internet router that can immediately identify the dropped connection and automatically fail over to the secondary connection.

Also, when bringing in a second provider, find out how it delivers its Internet service and make sure it is through a different pipeline than your primary provider. If both of your providers deliver Internet using underground lines and those lines are severed, you will not have either connection.[4]

Monitoring & Patch Management

Having a provider or system to monitor your network (including your servers and workstations) will enable alerts to be

sent when systems are about to fail or when there has been a network intrusion. Patch management keeps your computers healthy and up-to-date with the latest operating system updates as released by the manufacturers. (For example, Microsoft releases patches every Tuesday, with a path management system to ensure they are successfully installed.)

Security Breach Protection

Install and configure a firewall that has intrusion prevention software to keep unwanted users away. Some Internet routers come with a built-in firewall and software to handle this for you, as well as a failover solution for redundant Internet connections. Ask your provider about the different options.

Antivirus, Anti-Spyware & Anti-Spam

Viruses usually infect one computer and can spread through all computers in your network, destroy data, and compromise your business information. They can come via e-mail or be downloaded from an untrusted website. Designed to collect information without appropriate notice or consent, spyware is usually downloaded from an e-mail attachment or installed on your computer when you follow an unknown link from an unknown sender or download software from the Internet. Spam messages not only crowd your inbox with unwanted advertisements, but can also be dangerous due to the content they carry (e.g., viruses or spyware).

We highly recommend an enterprise-managed solution that includes antivirus, anti-spyware, and anti-spam and that these protections are updated daily in all computers, wireless devices, and servers in your network.

Alternate Plans in Case of an Outage

Your disaster recovery plan should include worst-case scenarios. Your company should have contingency plans to continue working without computers in case nothing is available for the short term.

Another option is to have your employees work from home or other alternate locations. With cloud services, much of your data could be accessible from a basic Internet connection, and your employees could use cellular phones or other communication devices to stay in touch during the outage.

Today's technology can offer some flexibility to a standard work environment; being prepared to use that flexibility is a big step in the right direction to stay in operation during a major outage.

External Resources

Once you have determined the acceptable downtime your company can handle, and gone through the checklist of best practices to see what is already in place, consider partnering with an IT provider that can meet your requirements and work as an extension of your team.

Make time to sit down with your IT provider to discuss key investment selection metrics[5] and most importantly your expectations. Ask key employees for specific feedback on the challenges they encounter every day, and make sure that the new solution you are putting into place addresses all of them and can be properly managed.

Conclusion

Downtime and security threats cannot be 100% prevented, but they can be minimized through a comprehensive approach that will prepare you and your staff in case of disaster. Planning for the possibility of downtime is the first step in keeping your business operational. It will also provide greater insight into the systems already in place and how they can be better used in your business.

There are many tools available to assist with this, including cloud computing and virtualization. Spend time with technology professionals to come up with a comprehensive plan. Since systems will change over time, review this plan annually. Just like setting budgets and financial forecasts, your business will benefit from this type of planning and review. ■

Endnotes

1. *www.megapath.com/megapath/assets/File/PDF/WhitePapers/WP_AffectsOfDowntime.pdf.*
2. Ibid.
3. Ibid.
4. *stimulustech.com/technology-tips/stimulus-technologies-true-redundancy.*
5. The Uptime Institute has a methodology referred to as FORCSS that comprises six key selection metrics designed to ensure effective investment by providing a holistic but succinct evaluation framework for key alternatives intended to avoid "analysis paralysis." (*www.symposium.uptimeinstitute.com/schedule/1860-forcss-session-2013.*)

NATHAN WHITTACRE is President and CEO of Stimulus Technologies in Henderson, NV, where he provides managed IT Services, custom computer design and assembly, diagnostics and repair of computer systems, and computer network design and installation.

Nathan earned a BS and MS in Computer Science from the University of Nevada Las Vegas.

Phone: 702-564-3166, ext. 1111
E-Mail: nathan@stimulustech.com
Website: stimulustech.com