ERADICATING FAILURE

Addressing Executive Management's Fear of Downed Networks



The Catch-22 Of Technological Dependency

For the past two decades, advancing technology has unquestionably enhanced the way we conduct day-to-day business. A stable, reliable and secure IT system means efficient operations and optimized productivity, service, and communications. It fosters greater opportunity and increased revenue potential. Today, through technology, small-to-medium sized businesses anywhere can serve customers globally twenty-four hours a day, seven days a week, which was unfathomable 5-10 years ago. In today's business world, anyone can be as big as they want to be.

This greater dependency on technology also presents a paradox in the sense that the consequences of network failure can often be fatal to small and medium-sized businesses (SMBs).

While system outages and failures can result in service hiccups and lost profits for large companies like Blackberry, Intuit, or Virgin Blue, these companies typically have enough resources to bounce back and continue on with business as usual once the underlying issue is resolved. Smaller and midsize companies don't have this same luxury.

For example, if a law firm pays $20,000 to recover from an email virus that corrupts their client data, or an online nutritional supplement company shells out $40,000 for data recovery and repairs after hard drive failure takes them offline for ten days, these companies are dealt a significant fiscal blow that they may never recover from.

ERADICATING FAILURE

The *National Archives & Records Administration* in Washington found that 93% of SMBs file for bankruptcy within twelve months of experiencing data loss and prolonged downtime of ten or more days.



Be Aware and Prepared... Not Overwhelmed

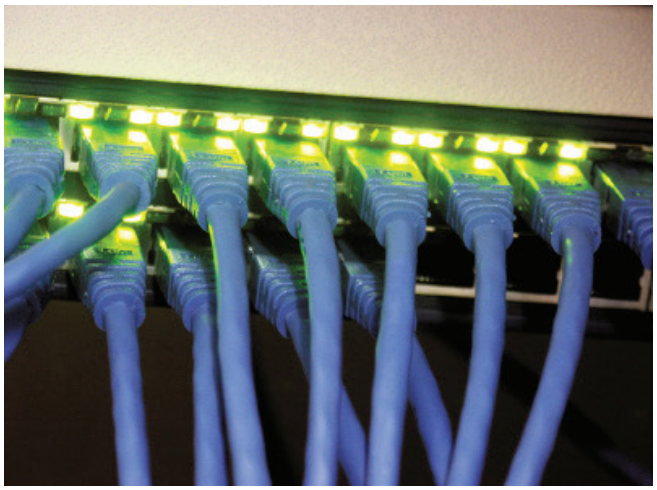
While the threat of **data center loss and downtime** is acknowledged, ask a group of SMBs how much they lose annually from network and system failure and you're likely to be met with many blank stares and wild guesses. Perhaps they can sound off the hourly rate they've been charged for IT services, or what they've recently paid to repair or upgrade software and hardware, but very few can even venture to guess how much is lost in productivity, revenue, services and customer goodwill.

The Aberdeen Group (an IT research firm) recently projected the estimated annual cost of downtime to be $25,806 for every small business employing less than one hundred people. Medium-sized businesses, employing anywhere between one hundred to one thousand employees, were hit even harder by failed technology at an estimated $880,600 per year.

Is it any wonder why many smart business owners these days aren't sleeping soundly at night? They're stressing over something they feel powerless to address - the stability and efficiency of their IT system and network.

But you aren't powerless as you may think. **Most IT system failures can be totally avoided, or reduced in severity, quite easily and inexpensively**. All it takes is some risk assessment, a plan, proactive maintenance and the right sizing of your legacy IT budget.

ERADICATING FAILURE



Can You Really Afford the Status Quo?

A successful SMB must align its technology and business initiatives. Constant employee productivity must be maintained to meet the needs and expectations of customers. To successfully do this, an honest assessment of risk is necessary. Regrettably, many SMB owners or management teams remain in state of denial that mismanaged technology has any serious consequences on their business. Meanwhile, it is costing them every day!

According to *Symantec SMB*, 50% of SMBs admit to having no backup and disaster recovery plan in place. Forty-one percent of those surveyed confessed that they had never even given much thought to implementing a disaster recovery or business continuity plan.

Every day SMBs are gambling with the lifeline of their business. Some may know they're playing with fire but budget limitations may prevent SMBs from hiring adequate internal IT support. Often, the IT support that is on payroll is overburdened and stuck in a constant reactive mode where they spend their days resolving issues that are already hindering productivity and service. They can never break this cycle to get to a point where they're actually proactively approaching things.

This same "break/fix" mentality is also the reason why many SMBs aren't hiring in-house IT support. They instead phone in expensive "as needed" emergency IT support when issues arise. There are so many smaller businesses and organizations needlessly bleeding money every day by subjecting themselves to the high hourly rates, service charges, trip fees and wait times of on-call IT support.

This is the status quo. Management cuts corners because they either feel they have no choice given today's economy or they're completely ignorant to the daily revenue being lost by mismanaged

ERADICATING FAILURE

business technology. Some know this will prove to be a costly mistake but they have no real vision to what it is already costing them every day.

Many SMBs don't have a healthy fear of technology failure. Nor do they spend much time thinking about the true return on their IT investment. SMBs must ask themselves a few questions to determine if their business can really afford the "status quo."

- How often is employee productivity and customer accessibility or service stalled each day from a downed network or system?

- How much downtime can your business truly afford and what kind of backup or recovery solutions are in effect when systems are unavailable?

- What level of IT support can be accessed? Can it be accessed quickly enough to minimize damage? Are you confident that your business can either be back online or be able to access lost data with minimal disruption no matter what?

- Is your most critical data frequently backed up? Is the data on the personal laptops, iPads or Blackberrys of employees backed up? Are all backups stored in a location off-site and quickly accessible in the event of theft, fire or flooding? Are you using any custom installed software and is the supplier still in business should this software need to be reinstalled or updated? Are account details, licensing agreements, and security settings somewhere on record?

- Are your systems truly protected from theft, hackers, and viruses? Are passwords to sensitive data changed whenever employees leave the company or organization?

- When was the last time you tested backup processes to ensure they are working properly? How quick were you back up?

ERADICATING FAILURE



5 Things SMBs Can Do Right Now To Preserve Their Network and Systems

1 Backup Files Every Day - The number of businesses that never backup their network is astonishing. According to the Symantec SMB data, only 23% of SMBs are backing up their data daily. Fewer than 50% are backing up data weekly. A number of events can result in data loss. The importance of frequently backing up your network cannot be overstated.

2 Ensure Backup Procedures Are Checked Regularly - Many times business owners think they have a backup system in place only to find out when its too late that it hasn't been working properly. It may seem like files are being backed up daily, however, the backup has become corrupt or huge chunks of critical data aren't backed up. Check backup procedures regularly to make sure they are working properly. Be sure that ALL data can be recovered. In this age of BYOD (Bring-Your-Own-Devices) it is also important to frequently backup data on the personal laptops, iPads or Blackberrys of employees.

3 Make Sure Updated Virus Protection and Firewalls Are Always Enabled - Far too many companies either have no virus protection software installed, expired virus software licenses, or disabled virus programs that aren't running at all. This makes their business technology vulnerable to virus attacks from emails, spam, data downloads, and other web sites. Files corrupted by a virus won't only bring down your network but if the virus is somehow spread to customers and e-mail contacts it's a surefire way damage your reputation as well.

Roughly 40% of small-to-medium sized businesses will have their network compromised by a hacker. Chances are, they will have no clue whatsoever that they were attacked. Hackers look online for unprotected and open ports and then infiltrate whatever space they can with malicious code and files. If this malicious

code cannot be removed, the hard drive will have to be reformatted and all files could potentially be lost. This is another reason why file backup is so critical in today's business world.

Updating critical security patches and changing passwords on the departure of employees are also necessary to deter hacking attempts.

4 Monitor Server Drives - Dangerously full server drives can bring on a slew of problems, ranging from program and server crashes to sluggish email delivery. Some proactive monitoring and maintenance of the server can spare businesses a lot of problems down the road.

5 Regularly Check Critical Built-In Logs - Very few tech problems emerge suddenly overnight. They typically progress and worsen over time into a more serious problem. Frequently reviewing the critical built-in log files can often indicate something is amiss before it becomes a major problem that wrecks havoc on your business infrastructure.



The Benefit of Managed Cloud Migration for SMBs

Many SMBs today are turning to cloud-based services and virtualized backup solutions as a means to mitigate downtime and recover from network failures and outages. Virtualization and cloud computing have enabled cost-efficient improved business continuity by allowing entire servers to be grouped into one software bundle or virtual server – this includes all data, operating systems, applications, and patches. This simplifies the backup process and allows for quick data restoration when needed. But migrating to the cloud or a virtualization infrastructure must also be handled with care as these new technologies still pose significant risk.

ERADICATING FAILURE

While virtual resources and hosted services reduce overall business technology expenses and improve availability, “managed cloud migration” allows for a gradual integration of a company or organization’s IT infrastructure and virtual data center to the cloud. This can alleviate many of the security and privacy fears that come with moving to a shared space while offering a more varied approach to recovery processes with more customization and control.

For Additional Information Please Contact
Scott Gallupe
scott@403tech.com
T: 1-888-270-9053
20, 805 5 Ave SW, Calgary, AB, T2P 0N6
https://www.403tech.com/