

# THE FAB FOUR:

## WHAT EVERY BUSINESS NEEDS TO KNOW ABOUT THEIR IT

---

### IT THAT WORKS

IT is frustrating. Confusing. A necessary evil. However you feel about IT, the truth is that for the vast majority of businesses, it's essential to the success of your organization. You simply must have IT that works.

But what does IT that works mean? Yes your computer needs to turn on, and you can't have it crashing frequently. However, we all know that there is much more to IT than what is in front of us every day. This is what most non-technical business owners try not to think about, because if we assume it's ok, it probably is, right? Actually, 92% of Chicago area small and mid-sized businesses have at least one major, potentially destructive, issue with their IT.

The "behind the scenes" of IT doesn't have to be overwhelming or unsettling. In fact, just by learning four simple aspects of business IT you can feel empowered to talk to your IT partner and ask if you have IT that works.

### NUMBER ONE: POWER MANAGEMENT

**WHAT IS IT?** Power management is incredibly fundamental to safe and secure IT, but frequently neglected. Power management entails having an automated and monitored Uninterruptible Power Supply (UPS). This kind of UPS will allow your servers, other equipment, and data to be safe in the case of a power outage. With UPS, when you lose power (on average once per quarter) a backup power

supply instantaneously turns on (which means your machines don't crash). This power supply lasts for five to 15 minutes, generally enough time for the main power supply to come back on. If the main power supply has not yet been restored, the UPS will allow your equipment to gracefully shut down. All you need to do is wait for the power to come back on, and all will be well.

**WHAT IF I DON'T HAVE IT?** If you do not have UPS, or if your UPS is not properly monitored to make sure it's working and automated, your risks are serious. Your systems could "crash", leaving you exposed to data losses, corruptions, even physical damage to the servers. If your backups are perfect, the best case recovery period would be about a full business day. If your backups are poor or non-existent (see Number 4), your road to a full recovery could be a few days, weeks, or never.

### NUMBER TWO: DISK REDUNDANCY (RAID)

**WHAT IS IT?** Your company's data is stored on a disk or disks. Disk drives tend to be fragile, and defects naturally occur every two to five years. This is a problem and can put your data at risk. To combat that risk, RAID, or Redundant Array of Independent Disks, is employed. Using RAID allows your data to be duplicated or spread across many disks. This means that if a drive fails (which is very likely to occur at some point) it will not interrupt business. Assuming your RAID is properly monitored, your IT partner will receive a notification and will then provision a new disk. No harm done, and no losses suffered. It should be noted that proper monitoring is crucial with

RAID. Without it, all your drives could have failed and no one would ever know – thus making RAID useless.

**WHAT IF I DON'T HAVE IT?** Without properly monitored RAID your disks could break (due to a natural failure or an electrical or mechanical shock). You may face a loss of data or a corruption. It could take several days to provision a new disk and if your backups are not perfect, some data might not be restored.

### NUMBER THREE: MALWARE PROTECTION

**WHAT IS IT?** Malware is something that can infect your computer or IT environment. It can take the form of a virus, trojans, spyware, root kits, spam or worms. Malware seeks out the vulnerabilities in your environment and can cause significant damage. Proper malware protection is not easy, and usually requires several layers and pieces to properly secure your environment. You not only need an trustworthy antivirus and spyware product, but you also need monitoring to ensure it is operating correctly. Antivirus is also regularly updated, but these updates have to be applied. You need an automatic system for application to ensure they occur. Depending on your environment, you may wish to employ email and web filtering to prevent employees from visiting specific web sites. In particular, all businesses need to actively educate their employee base to understand the dangers of malware, and the damage it can cause.

**WHAT IF I DON'T HAVE IT?** Chances are you would never risk not having any malware protection whatsoever. However, you very well may not have effective malware protection or enough malware protection. We have found that at least one third of Chicago area small and mid-sized businesses have no protection, and the majority aren't sufficiently protected. Risks of poor protection include identity and fiduciary theft, collateral damages, data loss, corruptions, and mild to extreme slowness of systems (resulting in an inefficient workforce and loss in productivity).

## NUMBER FOUR: BACKUPS

**WHAT IS IT?** If any of the previous Fab Four are flawed even slightly in your business, you should immediately check to see if your backups are perfect. Backups are like business liability insurance. You hope you will never need them, but if you don't have them when you do – your business could be ruined. What's startling is that most companies believe they have backups. They may even have a good reason why they believe that. But less than 50 percent actually have working backups. What that means is that if you have a power failure, a catastrophe, or a rogue employee who destroys files – all your important and unimportant files could be completely lost. 50 percent of small and mid-sized businesses who experience a major data loss do not survive. It is completely crucial to the success of your business that you have full backups that you know will work.

In order to accomplish this, you need a backup strategy. This may include local backups that you rotate, remote backups that are stored in the cloud, an image based backup solution, and a Disaster and Recovery plan.

**WHAT IF I DON'T HAVE IT?** Without full, verifiable backups of all your essential data your entire business is at risk. There are very few companies that can survive

without their financial data, proprietary plans or information, etc. And there is always other data that is just annoying to lose and have to replicate. You need a backup solution that is robust and tailored to your business, as well as monitoring to ensure it actually works. Don't assume it's working – backups fail with regularity.

## THE BOTTOM LINE

### WHAT NEXT?

At the end of the day, you don't want to worry about your IT. You don't want to wonder if your RAID is being monitored properly, or if your UPS will work properly if there is a power outage. The bottom line is that your IT should be your partner, not a constant liability. Your IT, when safe and secure, can help propel you to meet your business goals. But that won't happen if you aren't informed on the basics of secure and reliable business IT.

Talk to your IT partner. Ask them to provide proof that your "Fab Four" are in good shape. Then ask them what's next for your IT? What else can your IT do for your business.