Here are a handful of blogs out of over fifty I wrote for clients of TSL Marketing. I've had to delete the client's names for legal purposes.

Is Your Infrastructure Converged, Integrated or What?

There is much talk in the tech industry these days about “converged infrastructure”. It’s an apt and accurate description for systems that have all the hardware and software elements of the IT infrastructure – compute, networking, storage, virtualization - built into one, pre-configured rack-in-a-box and managed from a central console. Every big vendor has one.

While the “converged” category of systems was being pushed to market, there was a little branding war going on behind the scenes. Cisco, HP, Dell and others were pushing converged infrastructure offerings, and IBM was pushing “expert, integrated systems”. Their PureSystems family of offerings was and is as converged as any competing system, except for one little word : “expert”. IBM PureSystems learn as they process, automating repetitive management and deployment tasks.

Today, the IBM PureFlex system sits squarely in the “converged” category, albeit sort of retroactively. In any branding war, one side will eventually dominate. Today it’s probably safe to say that “converged” outgunned “expert, integrated”, and IBM has had to follow suit to avoid being overlooked. As if Big Blue could possibly be “overlooked.”

On average, purveyors of converged infrastructure systems claim that clients can expect to achieve 20-30 percent improvements in deployment times, utilization and staff productivity. PureFlex clients are achieving far better results:

- · Services can be activated in minutes or hours rather than days or weeks,
- · 47 percent reduction in time related to system management
- · Utilization up by 25 percent
- · Reduced downtime by up to 97 percent

Impressive, right? To be fair, there are other important things to consider when evaluating a converged system. First, as with any all-one solution, you’re locking into one provider. If you want to modify the system, your choices will be limited. That is if you can modify the system at all. As the IT Green Pagesputs it : “The land of Converged Infrastructure is much more a dictatorship than a democracy. You will have some choices from a configuration aspect, but nothing close to the choices you would have going with a piece/part solution.” In other words a converged infrastructure system is not for those that like to tinker.

One of the great things about engaging with the IBM experts at XXX Systems is the breadth of IBM products they support. If a converged PureFlex system isn’t a perfect

fit for your business, American Technology Systems will work with you to come up with the right combination of hardware, software and services to help you maximize your investment in technology. To learn more contact the IT specialists at XXX Systems.

Are You Ready for Old Man Winter?

Old Man Winter has arrived and boy is he mad. Hopping mad. “No more Mr. Nice Guy!” he declared in a recent pummeling of the west with 4 days of solid rain, snow, high winds, floods, power outages – all the things Old Man Winter is famous for.

According to AccuWeather, the northeast and southeast regions will be hit hard in the first quarter. The Farmers’ Almanac predicts this winter will bring below-normal temperatures for three-quarters of the nation. Predictions are so dire that the Federal Emergency Management Agency (FEMA) recently released a winter preparedness guide for U.S. citizens. They did not, however, provide a similar guide for beleaguered IT managers with Old Man Winter on their minds.

In the IT department, disaster recovery goes hand-in-hand with high availability. Should your business be hit with a disaster—bad weather, service outage, or human error—you want to be able to recover the data that is critical to your continued operation instantly. In order to do that it must be “highly available”. According to TechTarget, high availability refers to a system or component that is continuously operational for a desirably long length of time. Availability can be measured relative to "100% operational" or "never failing." A widely-held but difficult-to-achieve standard of availability for a system or product is known as "five 9s" (99.999 percent) availability.”

For a high availability solution to be effective, it needs to be incorporated into a bulletproof plan. Essential elements of your disaster recovery plan should include:

- Data classification or tiering - by classifying your data into tiers of importance, you determine which applications and data get recovered first, second and on down the line to data you can afford to live without. In the process you define the recovery point objective (RPO) and the recovery time objective (RTO) for each tier of data, and the cost of recovery. Lower RPO-RTO = higher cost.
- Replication - redundancy and/or co-location – having the same data in two places at once - is the most basic tenet of all disaster recovery plans.
- Timing - specify how much data you need to recover, and how quickly, in order to get back up and running.
- Testing - you can’t over test a disaster recovery plan; it is the only way to know if your plan will work. Test at least once a quarter; parameters and variables change quickly and what worked today may not work three months from now. TechTarget provides a concise guide to disaster recovery planning should you wish to learn more.

The disaster recovery and high availability experts at XXX Systems can provide solutions that are ready to scale and can handle any challenge, on any platform, in any combination of physical, virtual or cloud servers. They'll help develop your plan and ensure you have the right tools to beat back old man winter when he comes knocking. For a free evaluation, get in touch with XXX Systems.

When Do-It-Yourself Does More Harm Than Good

Small and medium business owners are a culture of figure-it-outers. When faced with a complex problem, entrepreneurial types are apt to rhetorically ask: "How hard can it be?" Often it's not until we've got parts all over the floor that the real answer occurs to us: it can be really, really hard. Why do we let ourselves get into such quandaries?

In two words: control and trust.

In a world where commerce can literally come to a screaming halt when IT systems go down, it seems unnatural to hand control over to someone else, then trusting they'll do the right thing. As a recent Information Week article puts it:
"[Many SMBs] believe that they cannot truly commit to trusting critical systems to an outside partner…This response defies logic, however. When faced with a critical operation or process, common sense dictates that trust is best placed in the hands of experts. Performing surgery on one's self doesn't alleviate the risk of a procedure going badly! Therefore, the adage, 'if you want something done well, do it yourself,' carries only so far."
Such sentiments at least partially account for the huge boom in the Managed Services business. As companies recognize that managing the IT infrastructure in house can turn into a sinkhole of unforeseen costs, they're turning varying levels of control over to Managed Service Providers. Some of the services MSPs can provide include:

- Off-premise Cloud Services
- On-site Management
- Proactive Remote Monitoring
- Desktop Management
- System Health Checks

The best MSPs will build-to-suit, allowing businesses to mix, match, and scale services so the solution delivers optimal ROI and maximum value. And while choosing the right MSP for your business is a topic for another day, some preliminary situation analysis can be an excellent way to prepare. According to Forbes, one approach is to "…take a step back and build a business architecture diagram that lays out the core business services that your company offers. Then draw up a reference architecture that depicts

all of the different IT services that are required to support those business services. Then, identify which of those IT services are core to your business and build those. Everything else should be outsourced to managed service providers or to various external services and products."

This analysis will be a good starting point for your conversations with MSPs. It's also a process that a good MSP can facilitate.

A one-stop shop like XXX can provide such an assessment and determine which options make the greatest financial sense. You may decide to sign up for Off-Premise Cloud Services package for one flat, monthly rate and give up tinkering with IT altogether. The important thing is to find a solution that fits your business model and lets you determine your level of IT involvement. Then you can decide whether you want to spend your time figuring out your IT systems or figuring out how to run a profitable business.

Don't Be Another Lost Data Sob Story

Everybody has at least one lost data horror story, individuals and business alike. Whether data is lost to a natural disaster, a system outage, or human error it can be disastrous. About 40 percent of SMBs affected by a big disaster never reopen.

In this era of public cloud providers like Amazon, Microsoft, and Google giving away storage in 10 or 15 Gb chunks, apathetic organizations have run out of excuses for losing data. With the arrival of big winter storms and other unexpected events, smart organizations are double-checking their disaster recovery plans to ensure that they won't get knocked out of business. However, many SMBs are not backing up their critical data to the cloud or some other remote site.

Outsourcing Disasters? What a Concept!

Some companies are now outsourcing backup and recovery services, which are also referred to as DRaaS (Disaster Recovery as a Service). For businesses that use their own internal data centers for primary storage, there are a variety of alternatives for backup and recovery. These services vary between those that replicate your infrastructure only, leaving recovery up to you, and turnkey approaches that both protect and recover your data. Regardless of the approach, every business needs to start with a plan.

When developing your disaster recovery plan, Information Week suggests these five basic steps:

1. Engage with a Managed Services Provider (MSP). If you already have one, make sure they can support your backup and recovery requirements.
2. Prioritize your web-based applications according to their importance to your business (also known as "data-tiering").

3. Virtualize your critical systems in the cloud or at a secure offsite location.
4. Ensure that a failure in your data center will be detected and will redirect users to the backup.
5. Test, test, and test again.

Enlist the Experts

While there are few things you can do to prevent plagues of locusts, system malfunctions, or human error, there is no shortage of information to help prepare for them. Articles describing the various steps you should take to ensure your business has a robust disaster recovery plan are plentiful.

One of the many services offered by XXX Technologies is data storage, along with managed backup and recovery for SMBs and large enterprises alike. Your business may benefit from regular remote backup of your virtualized data to a public, private, or hybrid cloud for high-performance tiered storage, live archiving, cloud-based data protection, and recovery. The storage experts at XXX Technologies will help put together your plan, implement a solution, run test scenarios, and provide ongoing management.

Contact us to learn how our storage and data backup solutions can improve your business functions and plan for the future.

Five Cloud Migration Myths Put to Rest

So you're thinking about migrating your business IT to the cloud, but you've heard that it can be a risky proposition, especially in Alaska where it seems the Internet has had connectivity challenges over the past several years. Sure, early adopters may have run into a few snags, and there are plenty of do-it-yourselfers out there that have undoubtedly gotten in over their heads.

Many of the mythical risks of cloud computing are simply ghosts from the past. For example:

1. **Cloud computing isn't as secure as my in-house data center**

Then why are 94 percent of organizations running applications or experimenting with infrastructure-as-a-service in the cloud? (Rightscale 2014 survey) As IT Business Edge puts it: "the cloud offers safeguards that traditional solutions do not. With cloud-based services, additional layers of protection are not only available – they are a priority for top providers. To succeed in the cloud market, security is paramount. Vendors know they need to provide trusted and secure cloud services to their customers."

2. My customers are based in Alaska. Local = faster.

The Alaska Business Monthly points out that "when your customer tries to access your website, the data request is usually routed Outside where the handoff is made before being sent back up to Alaska. Then, the data response from your server heads back down on a second round trip before arriving at your customer's computer. This double round trip is made a bajillion times every time you load a webpage. The irony: by placing your servers in the Lower 48, they could be twice as fast as having the servers in Alaska."

3. Internet connectivity between Alaska and the Lower 48 is unreliable.
There are four distinct fiber pathways between Alaska and the Pacific Northwest and not a single point of failure that would affect all four. If one goes down, the next one picks up the transmission. Plus the state government has mandated more. Connectivity is reliable now and will only get better.

4. Data migration is fraught with peril – data is sure to be lost

Whether you are transitioning all or part of your company's data, applications and services from on-site to the cloud, your provider will be using tools that will seamlessly migrate your data to their servers. As Business2Community.com puts it: "If MSPs are good at one thing, it's planning migrations."

5. In the Cloud, I lose control over my enterprise data and my IT infrastructure
Actually, you'll gain greater control over your data and your infrastructure when it's hosted by an MSP, either in the cloud or on their systems. The only difference is that somebody else is doing the work on your behalf.

Still have doubts? The XXX Managed Services team would be happy to assess your organization's cloud readiness. You can contact us here.

Three Approaches to Managing Mobile Workforce Technology

One of the more dramatic shifts in enterprise computing has been the phenomenon known as BYOD (Bring Your Own Device). On one hand, the fact that employees are willing to use their own bought and paid for mobile devices to do company business is a win-win for everybody. On the other hand, now you've got employees accessing the company network from, well…anywhere.

As an article in NetworkWorld puts it, "The future of end user computing is here today… and it's in your pocket. And your house, your office, and your favorite seat on the 8 a.m. train. It's wherever you are."

In other words, if there's one key trend that is affecting the workplace, and it's that the workplace itself is fast becoming an anachronism. Not only do workers want to be able

to work from wherever, they want to use the devices and the applications of their choosing. Here is a look at three ways the industry is addressing the IT challenges of the mobile enterprise.

1. Take Back Control

The control, security, and data privacy concerns have prompted some companies to provide mobile devices to their workforce. According to an InformationWeek report:

- The number of companies providing desktop systems to more than 50% of the workforce has dropped from 68% to 54% in the past three years
- Over the same period, the number of companies providing iPhones and Android devices to the workforce went from 2% to 20%
- Distribution of thin client Virtual Desktop Infrastructure (VDI) rose from 4% to 11% (40% have VDI in production)
- 61% of organizations surveyed now provide technical support for employee owned devices

While company-issued mobile devices may provide some level of built-in security and control, it is an expensive solution. More expensive than the costs associated with an office full of PCs? Ostensibly, no. But it depends on the company.

2. Enter the Personal Cloud

Another trend that is intended to enable the mobile workforce is the idea of the personal cloud. According to John Fanelli from Citrix, a personal cloud can provides secure, instant access to the apps, data and people necessary to get work done from any device, anywhere. The model assumes that apps will increasingly be delivered as cloud services - whether private or public – and procured through enterprise app stores. In the personal cloud environment, every worker's files and apps are easy to access, share and secure on any device.

3. The Resource Hub

A third approach, as discussed by Brian Grimmage in a NetworkWorld article, involves managing resources at the point where they are accessed, as opposed to managing the devices as individual assets operating within a standardized configuration. Grimmage envisions an enterprise hub that manages the resources users connect and access regardless of the type of device being used.

At this point, the only universal agreement is that BYOD is here to stay and that there is no one silver bullet that will satisfy the need for security and control. How are these trends affecting your organization? What approach will you take to mitigate the inherent risks of the mobile workforce?

At XXX, we're engaged in related conversations with customers of all sizes from a variety of industries. Let us help you navigate possible solutions for your growing mobile workforce.