



SMB Newsletter

Issue 43

133 Cromwell Lane
West Chester, PA 19380
610.429.3122
www.ladenterprizes.com
info@ladenterprizes.com

Our first newsletter of a New Year highlights the current information technology trends. In the past we included information based on surveys and research by industry research firms as well as our own opinion. The trends also had a tendency to be hardware or software related. This year with the economic downturn, the key trends we are hearing about and seeing businesses implement tend to be more business oriented with technology being looked at as an “enabler”.

The **2009 Trends** or thought processes around information technology are somewhat different than the past.

As we move forward in 2009, our SMB Newsletters will continue with our “What is” and “Keep IT Simple” series as well as other topics we think businesses may find interesting. For people who have asked -- Yes, the “Keep IT Simple” recommendations are Best Practices. Past “What is” and “Keep IT Simple” series articles can be found on our website, www.ladenterprizes.com.

David Burford

Laura Dallas Burford

Inside this issue:

2009 TRENDS— DIFFERENT THAN THE PAST	1
A BALANCING ACT – DRP AND BCP	2
IT OUTSOURCING— THE GOLDILOCKS STRATEGY	3
WHAT IS A FIREWALL ?	4
KEEP IT SIMPLE TIP: CONSIDER WARRANTIES FOR HARDWARE	5
SMALL BUSINESS TECHNOLOGY PLANS	6
FOOD FOR THOUGHT	6

2009 Trends – Different than the Past

The economic downturn is forcing businesses to reevaluate spending, business processes, currently implemented (or not implemented) software and hardware solutions, and new technology initiatives.

Over the past 10 years, Information Technology has become more embedded in business and key leaders realize technology is the “enabler” to help them survive or move forward. Key leaders are looking for technology solutions that meet the business’s strategy, integrate applications, and deliver what is expected and needed. Users and customers have become tech-savvy and expect businesses to use technology to deliver results. The intertwining of business and information technology has become a necessity.

As we reviewed the 2009 trends, we noted an emphasis on as well as intertwining of

business and information technology. A number of articles in prior newsletters related to the trends, therefore some related articles have been noted. The key 2009 trends are:

Align information technology with business strategy. By looking at the “total picture”, it is possible to align your business processes and Information Technology needs with the overall strategy and goals of your organization. Consider reading: [View of Information Technology’s Relationship to Business](http://www.ladenterprizes.com/pdf/View_of_Information_Technology’s_Relationship_to_Business), (www.ladenterprizes.com/pdf/View_IT_Relation_Business.pdf)

Reduce IT operating expenses. Virtualization, eliminate unused resources, and outsource technology management are just some of the approaches to reduce expenses.

(Continued on page 2)

(Continued from page 1)

Consider reading: [Virtualization -- Is it Right for You?](http://www.ladenterprizes.com/pdf/Virtualization.pdf) (www.ladenterprizes.com/pdf/Virtualization.pdf); [Optimize Your IT Costs](http://www.ladenterprizes.com/Optimize_IT_Costs.htm) (www.ladenterprizes.com/Optimize_IT_Costs.htm); [IT Outsourcing: The Goldilocks Strategy](http://online.wsj.com/article/SB122910537162602223.html#articleTabs%3Darticle) (online.wsj.com/article/SB122910537162602223.html#articleTabs%3Darticle)

Reduce the risk of information and technology-based disruption and understand how to restore the business. Backup, Disaster Recovery Plans and Business Continuity Plans all assist with reducing risk, but in some cases they help to reduce overall cost and improve efficiency. Consider reading: [A Balancing Act - - DRP and BCP](#) (see article below); [I've Been Told a Backup Procedure is a Must-5 Steps for Designing a Backup Process](#) (www.ladenterprizes.com/pdf/Backup.pdf)

Improve business processes to meet goals.

Changing how you are working can improved sales/fundraising, reduce the cost of manufacturing, and improve the delivery of current products or services. Consider reading: [Business and Technology – Working Together?](http://www.ladenterprizes.com/pdf/BusinessTechnology.pdf) (www.ladenterprizes.com/pdf/BusinessTechnology.pdf)

Increase the use of information technology to improve business performance and outperform competitors. New software and technology tools have created opportunities for companies to integrate technology into their business. To achieve this, software and technology tools need to be carefully decided upon, *planned* and then used effectively. Consider reading: [The Technology is Great, But is it Integrated?](http://www.ladenterprizes.com/technologyintegrated.htm); [Small Business Technology Plans -- Creating a Technology Plan for Your Business](http://www.gaebler.com/Technology-Planning-for-Small-Businesses.htm) (www.gaebler.com/Technology-Planning-for-Small-Businesses.htm)

A Balancing Act – Disaster Recovery Planning (DRP) and Business Continuity Planning (BCP)

Disasters and the resulting downtime could be hazardous to the financial well-being of a business. The challenge is many people think of disasters such as the Northeast Blackout (2003) or Hurricane Katrina (2005). Events of this magnitude are rare for the normal business. Local power failures, telecom failures, local flash floods, and actions by a disgruntled employee are the common challenge for the average business.

Some business owners, executive directors, board members and/or key employees think they will not experience a disaster. Businesses also normally take steps to protect and secure their application data, while few have prepared the organization to resume critical business processes within a desired timeframe. Some key people are surprised to find out that although they have backed up their application data, they still cannot resume business – they are still down and losing revenue.

Businesses cannot afford to lose application data and they cannot afford to have their network infrastructure down. It just costs too much to be down; to be unproductive. Think about:

How long you can survive if you do not have access to your primary applications and data; the internet; key client files; your email?

What is the impact on your bottom line if your office workers are not able to work; no orders are able to be received or processed?



For many small and midmarket organizations a full-blown Disaster Recovery Plan (**DRP**) or Business Continuity Plan (**BCP**) is more than they need and perhaps more than they can afford. Resources are limited; it is important to work smarter, not harder. It also is a **Balancing Act**.

If you do not have a DRP or BCP, here are a few action items to consider or to use my term, the “Emergency Checklist”. Please note, these action items do not take the place of a DRP or BCP.

“Whose in Charge”

During a regular staff meeting, spend time discussing

(Continued on page 3)

(Continued from page 2)

possible disasters and determine who should be responsible for what tasks during the disaster. Also assign a backup person for each task.

"You can't communicate, you can't recover"

Collect and maintain up-to-date contact information for your employees, vendors/suppliers and critical numbers such as Insurance contacts. Depending on your business, you might want to have contact information for your clients/customers. It is better for key clients/customer to hear there is a problem from you rather than from the news media.

Develop communication instructions and communications infrastructure. Develop a process for contacting your employees when an emergency occurs. Ensure your process is flexible and provides for more than one method of contact.

"Plan for no facility."

Plan for your local infrastructure to not be available. Determine before a disaster occurs a possible facility where the business can operate out of.

Determine what network and operational documentation is needed immediately for your business to operate. Try to keep the documentation as current as possible. This includes technology equipment lists, existing network diagrams and application manuals. Also prioritize and publish a recovery sequence to minimize the outage affects.

"What, no backup of data!"

It is one thing not to have a disaster recovery or business continuity plan, but at a minimum pertinent data should be backed up and maintained off-site along with the restore procedures. This is more than just

application data and files. Data for re-establishing routers and servers is important as well. For more on how to think about backup check out [5 Steps for Designing a Backup Process](#) on our website.

"I don't need to worry, I've outsourced my business application, website, etc."

If you have outsourced your data (a web application, customer relationship management system, etc.) consider a hosted service provider in another geographical region.

If the outsourced application is critical to your existence, understand the DRP and BCP of the vendor(s). If the vendor goes down due to a disaster, you might be down as well. Know their Service Level commitments to you if they incur a disaster. Ask to see their plan knowing they will not provide the entire plan to you. It is possible they will show a sanitized plan, a recap document or just some key information such as a generic description of the plan, plan creation date, last updated, last tested, etc.

"Expect the Unexpected"

Plan to not stick to your emergency plan.

No solution can provide 100% protection. Disasters as well as people are unpredictable. Be prepared for nothing to go according to plan and plan for change. Ad hoc decisions will need to be made.

During and immediately after a disaster, people do not have time to think — they need to act. Appropriate information needs to be readily available and stored offsite. Even if you have a softcopy, a printed copy of documentation is recommended. A computer may not be available to read the softcopy of the documentation.

IT OUTSOURCING: THE GOLDILOCKS STRATEGY (EXCERPT)

One Size Does Not Fit Everyone – You Need to Determine the Right Size for you. The same holds true for IT Contracts. A True Story and Good Article in the Wall Street Journal, December 15, 2008

.... "Not too lax. Not too rigid. A contract that falls somewhere in the middle is the one that works best when a company is turning over its information technology activities to an outside firm.

Contracts are critical to IT-outsourcing success because they help organize the relationship between client and



(Continued on page 4)

(Continued from page 3)

vendor, providing companies with protections against unwarranted fees and subpar service.

But contrary to popular belief, a contract that tries to anticipate and address every contingency that might arise during the course of a business relationship can be just as damaging as one that leaves too much to chance. It can create an atmosphere of distrust that saps a vendor's motivation to provide good service and go the extra mile when a client needs it most, such as when the business environment changes unexpectedly.

A look at the history of IT outsourcing at a French company between 1994 and 2007 shows the benefits of striking the right balance between "too little" and "too much" contract. The firm remains anonymous at its request.

A 'Standard' Contract...."

For the complete article – IT Outsourcing: The Goldilocks Strategy; (<http://online.wsj.com/article/SB122910537162602223.html#articleTabs%3Darticle>)

What is a Firewall? How Does It Work?

The most important function of a firewall is that it stops anyone on the outside from establishing a connection with a computer in your private network.

At its most simple level a firewall provides a way to filter information moving through the network connection. When present on an individual computer, it is called a personal firewall. Otherwise a firewall is used to protect computers on the "inside" network (your private network) from computers on the "outside", usually the Internet. Because of this, firewalls are usually included Internet gateway devices which may also have modem, router or switch functionality.

Firewalls allow or block communication between computers based upon rules. Each rule defines a specific network traffic pattern and the action to take when that pattern is detected. These rules are customizable. It is these customizable rules which provide control over the use of the network.

Note - A firewall only operates on communications traffic that physically passes through it. A firewall has no impact on traffic between two computers on the same "side" of the firewall (i.e., both connected to the same firewall port).

A firewall can be either a program (software) or device (hardware) and filter in-bound or out-bound network traffic. The Windows XP operating system firewall and Zone Alarm are examples of software firewalls.

SonicWall and Cisco Pix are examples of hardware firewall product lines.

How does it work?

A firewall works by blocking unsolicited traffic – anything your computer didn't specifically request. There are several methods used to filter traffic, which may be used individually or combined into a firewall product:

- Circuit level gateways,
- Packet Filtering,
- Stateful Inspection, and
- Proxy service also called Application Level Gateways.

What a firewall does not do is:

- Block or Disable viruses, worms or other malicious software.
- Provide protection from viruses or programs you download or e-mail attachments you open.
- Filter or block pop-up ads or junk e-mail
- Stop users from malicious or unsafe unapproved activities.
- Provide encrypted, encapsulated/tunneled communications or computer (host-to-host) authentication.

These functions require other technologies.

Some Final Thoughts

First, firewalls are not free. The more sophisticated/ functionally capable the firewall and its configuration the more expensive it is to acquire configure and maintain.

(Continued on page 5)

Second, effective firewall configuration requires technical expertise in network communication protocols. If you don't understand TCP/IP, you shouldn't try to configure a firewall.

Third, firewalls are an important component of any network but are not a security panacea. The most secure firewall is one that does not allow any traffic to pass – defeating the purpose of the network. Because firewalls can be a hindrance to effective use of technology, firewall rules must be realistic, permitting staff to use the network to fulfill desired functions, and should reflect the level of security in the entire network.

Last, for a firewall to work effectively, it must be a part of a consistent overall organizational security architecture/structure. Such architecture would include measures such as physical security, password policies, and use policies that spell out what can and cannot be done with organizational data, sharing logon information, E-mail or surfing web sites.

An expanded version of What is a Firewall including descriptions of methods used to filter traffic can be found at – www.ladenterprizes.com/What_firewall.htm

KEEP IT SIMPLE TIP: CONSIDER WARRANTIES FOR HARDWARE

Should you or should you not purchase warranty for your hardware? Is warranty a waste of your money? Aren't warranty programs a profit generator for the hardware companies?

Our advice

- Yes, purchase warranties for your hardware.
- No, it is not a waste of money.
- Yes, it is a profit generator for the companies.

But it is well worth spending extra dollars to obtain the warranty coverage. The coverage provides you with replacement parts and depending on the warranty, service if your workstation or server breaks.

Why do we recommend letting the hardware vendor replace the parts? It normally cost less. The vendor knows which parts will work with your hardware and if the part(s) does not work they take responsibility for obtaining the right part(s). We have even seen vendors

replace workstations when they are not able to properly repair workstations under warranty. If you need to hire a person to repair the hardware, the repair cost of a third-party is normally more than the original warranty cost and the person normally does not have access to the vendor related part information.



Working with Dell, Thomas L. Friedman (**The World is Flat**) traced the entire global supply chain that assembled his laptop. Including suppliers of suppliers about **400** companies in **3** continents (North America, Europe, and Asia) and **30** key players were involved.

For more information, check out Thomas L. Friedman's **The World is Flat**, Release 3.0, Chapter 16, The Dell Theory of Conflict Prevention.

SMALL BUSINESS TECHNOLOGY PLANS --

CREATING A TECHNOLOGY PLAN FOR YOUR BUSINESS (EXCERPT)

“Small business technology plans? There's no better way to make sure you're one of the many small businesses taking advantage of technology to outperform competitors and achieve efficient small business growth. If you fail to plan, you plan to fail!”

Trite, yes, but also true.

“...Technology is an unavoidable cost of doing business in the twenty-first century. Unless you have the proper technological resources, your company will quickly find itself lagging behind the competition....”

For the complete article –Creating a Technology Plan for Your Business; (<http://www.gaebler.com/Technology-Planning-for-Small-Businesses.htm>)

FOOD FOR THOUGHT

Late last year, I received a telephone call asking for our business address so that they (the organization) could send us a RFP for outsourced information technology support.

My first question: “Could I please set up an appointment on the decision maker’s calendar?”

Response: “No – there will be no interviews or clarifying meetings. If you have a question, send us an email. We want everyone to just respond to the RFP. We need to be able to perform a one to one comparison.”

Very quickly I realized that the business viewed their technical consultants only as implementers and input from implementers was not welcome. Technology was not being looked at as a strategic enabler.

Before you call an information technology consultant, know if you are looking for an implementer (implements what you have decided upon) or a strategic partner (implements but also participates in long-range, organizational strategic planning so that technology is used as an enabler).

More on this in our Next Newsletter.

Upcoming Seminars

.... To Be Announced

Look for our **Information Technology Leadership Series** coming later this year.

CEOs, Presidents, Owners, Executive Directors, Chief Financial Officers – **Business Leaders** – are not in their position because they know technology. Rather they are there because of their knowledge of the business and how to move the organization forward. Successful leaders need to know how to use and communicate information technology needs to their advantage. Information Technology needs to work for an organization and not the other way around.

Today no organization can exist without using and integrating information technology into the daily operation. A major challenge is leaders are educated in key concepts in areas such as finance, human resources, marketing and sales. They are taught how to create business plans, but many leaders have minimal knowledge of key information technology concepts including how their ability to communicate organizational needs impacts technology success or failure.

Through a series of seminars, we will discuss some of the information technology needs that a business leader needs to understand.

OUR SERVICES

NETWORK ENGINEERING (Network Technical Assessments and Planning, Local Area Network Implementation, Network Administration, Maintenance and Support)

INFORMATION TECHNOLOGY CONSULTATIVE SERVICES (Strategic Technical Business Planning, Software Selection and Implementation Assistance, Business Workflow Improvements, Disaster Recovery/Business Continuity Planning, Interim CIO)

Owner of **Computer Census™**

For More Information

Phone: 610-429-3122

E-mail: info@ladenterprizes.com

Website: www.ladenterprizes.com