A KDI White Paper

404 – 17768 65A Avenue
Surrey, BC V3S 5N4 CANADA

Call Toll Free: 1.800.661.1755
www.kdi.ca

Seven Key Ways to Find Out if Your Information Technology is Paying Off

January 2009

Not Sure About IT Value?

Ever look at your investments in Information Technology (IT) hardware, software and people, and wonder if they are actually paying off? This paper will show you **seven key measures** to find out whether you are really getting a quantifiable return on your IT. They are not difficult or time-consuming, and they will give you interesting answers. You'll probably understand better how IT components assist your business, too.

Yes, with very few exceptions, you need IT to be in business these days. Maybe if you're a shoe repair person in a one-man shop, you don't need IT. But in any business where you need to track customers, inventory, money, order parts from vendors, and a thousand other things, you have to have IT.

Right now you are in a unique IT situation. You have some IT components and you don't have others. Decisions whether to have a firewall, content filter, offsite data backup, someone to help you with IT issues or not has been based on education, knowledge, experience, 'gut feel', what your neighbour says or industry rumour. So how do you know whether you are **actually getting a measurable return on your investments in IT**, or are missing components you should be making use of? Let's look at seven clear IT value indicators.

1. Is Your Data Really Protected?

You have lots of data: client records, sales orders, purchase orders, accounting ledgers, maybe engineering drawings, graphic art or process control data. It's all being stored on a device called a server (if you're a larger firm) or on your networked PCs (if you're a small firm). Perhaps you even have a Virtual Private Network (VPN) and remote access, so that people can work from home or salespeople can access company files via their laptops when they're visiting clients.

Now the problem here is that this data is very important—without it, you can't run your business—and there are viruses and hackers that will damage it if they can. The IT component that is protecting your data by standing in their way is called the firewall.

A firewall protects your data when it is transferred over the Internet by doing something to it called encrypting it. Many firewalls follow the lead of online banking and encrypt data to the 128-bit level. A 2-bit increase in encryption level means your data is *four* times more secure—the square of the encryption, not double. The highest level of encryption is 256-bit: over one million times more secure than online banking. If you can get a firewall/VPN product that protects your data at that level, you should get it.

If you don't have a firewall at all…you need one.

So how do you know if your firewall is paying off? If you don't have a firewall, or its security level isn't good enough to stop hackers or viruses, your data will be corrupted or deleted and your network could go down. In those cases, you will not be able to do any business that requires Information Technology. Think about that: no business processes that require a computer or your network. No order entry, purchasing, accounting…you get the picture.

At that point you will have to get an expensive IT professional to come in and fix things. Your IT-driven business processes will be down for awhile. No income for that period. How long? Probably several days. How much does this hurt? Take your company's (or your business unit's, if you're not the owner) annual revenue. Divide it by 260. That'll give you your average revenue per day, assuming a 5-day work week. Sure, it's not perfect—it doesn't take into account seasonality, periodic promotions, big orders from one-time clients (what statisticians call 'outliers')—but it's useful for our purposes. You can even calculate a figure for revenue per *minute!*

Next, you want to take that revenue per day figure and multiply it by the number of days you estimate your network will be down and you won't be able to operate your business. OK, so you can revert to telephone and pen and paper and get some business done that way. Let's say 50%. So multiply the total figure you have so far by 0.5. After that, you'll add on an estimate for the cost of the IT expert to fix your network. We could get into things like a certain percentage of customers getting upset and leaving during the downtime period, but let's keep it simple. This total will be the base cost of the attack, if you don't have a good firewall. That's how much it hurts.

Example: From an annual revenue figure of $2,000,000, your average daily revenue is a little under $7,700. A virus hits your firewall-less network and your IT is down for three days while a tech works massive overtime to get everything back. At $90/hr for three 16-hour days, the tech costs $4,320. The interruption of revenue is $23,000 X 0.5 (because you can still run your business at half-tilt using pen and paper) and the total base cost of the attack is over $15,800.

During a three year-period, the standard service agreement for a firewall product, you're likely at risk to be attacked at least once a year.

When you consider that a good, high encryption-level firewall with lots of other useful features for network management costs under $5,000…you don't have to be a mathematician to see the return on investment. Over $47,500 vs. less than $5,000. *A No-Brainer, wouldn't you agree?*

This is how you tell if your firewall is creating value for you, and not just sitting there on a shelf blinking an LED occasionally.

2. Is Your Data Safe from Disaster or an "Oops!"?

Your network hardware can always be replaced, but data is something else. If data is damaged or gone, your business is in trouble. You can ensure your data is safe, though, but the kicker is that you have to have this solution in place before any problems happen.

If you don't have some form of offsite data backup and a recovery procedure, you need them.

Many people perform their own file backup. Most of the time it's done haphazardly, though: "When I remember about it"; "I forgot to the past two months" are common refrains. And here's a serious fault in this approach: a tape or drive with the backed up data on it left in your office *has no value*. If there's a fire or a flood, your backup is gone with everything else.

Data has to be securely stored **off site** in order to be safe. However, the monotony of bringing in and taking home a portable storage device every day is bound to lead to a breakdown in your procedure. Eventually, you're simply going to be too busy or forget…and *that's* the night something will go horribly wrong.

The best way to take care of file backup is to have someone else handle it. An expert, who knows about secure data transfer and storage. They can hook up a device that will automatically back up your files every night, without you having to remember or do anything. And when you need to recover a file, it's readily available because it's been stored off site.

See, when you buy a backup system, you're not buying backup. It's like when you buy a drill bit: you're not buying the drill bit, you're buying the hole it will make. Having backup tapes lying around your office is a waste. *When you buy a backup system, what you're really purchasing is the peace of mind of being able to easily recover your files.*

So how do you know whether your data backup system is paying off? If you don't have one, it's definitely not. If you do it yourself and leave the storage device at the office, it has very little value—only on the odd chance that you have to recover a file that was accidentally deleted…and you happen to have remembered to do the backup recently.

If you have a system that automatically backs up your data to secure, offsite storage every night, though, *then* you're getting value. It works like this:

In the case of disaster, you cry a little, find new offices, buy new hardware, and then easily download your files and get back into business. In the case of an "Oops!", like when you delete a client file by mistake, you easily download your file from the backup server and get back to work.

Without this ability, and remember that's what you're really paying for, you'll either be wiped out and have to start from zero…or you'll spend truly unnecessary time re-entering data to duplicate files and work you've already completed. The odd thing is, automated offsite data backup is one of the *simplest, cheapest and most effective* ways of ensuring business continuity and keeping your life sane, and just about everybody knows this—yet most people never bother to set such a system up.

Take the time you estimate it would take to rebuild a file. Multiply this figure by the average pay rate of the employee who would be doing the work. Then multiply this amount by the number of times a year you estimate an "Oops!" happens. This total is the benefit of having the data offsite and easily recovered. There are spillover benefits too, but we won't complicate matters now. Compare this with the annual cost of the data backup service.

Example: You have just accidentally deleted your client invoicing file (*F10* to Save, not F11, darn it!) for the engineering work you did over the last month. $22,000 and it needs to get invoiced today to get into the billing cycle so rent can be paid next month! "Oops!" Re-entering it will take about an hour, because it's so detailed and the client's A/R people are nitpicky…and you make $40/hr. The cost of you re-entering the invoicing file is $40, then. Over the year, you figure this happens once every couple of months. And it's not just you. The F10 key is right next to the F11 key, and one saves and the other deletes in your accounting system. There are four engineers working for you, at $30/hr, and they too hit the wrong key from time to time: the total annual cost of all this duplicate entry is $960.

A good automated offsite backup system should cost less than $100/month. That's under $1,200 a year, but you now know that the actual cost is less than a fifth that, because the easy file recovery feature saves you a lot of work. **And the value of the peace of mind is incalculable.**

The savings from the file recovery feature alone could easily total more than the service cost.

3. How Long Does Your Data Recovery Take?

Let's continue looking at automated offsite backup. Another way it saves you money is the speed at which it allows you to recover your data and get back to business. For example, what if a server with critical data on it fails and you can't enter parts orders, thereby delaying your customers from getting the products they need? That will take time to fix, and you'll be losing revenue all the while. The faster your data is recovered, the faster you'll be back to making money.

Example: You lose access to all of your parts database and ordering application when a server fails. Knowing your average daily revenue, you know you're losing over $1,500 a day when you can't serve all your customers—reduced to pen and paper as you are. Fortunately you have automated offsite data backup. Over the course of the day, techs buy and install a new server, then easily download the backed up files. Tomorrow, you'll be up and running at full speed again. Having the offsite backup service saved you at least another day of trying to get the database back together: that alone is worth more than the cost of the service.

4. Is Your Network Uptime Increasing?

Good firewall products have network management features, like traffic shaping and bandwidth monitoring. These tools allow you to be alerted to and home in on trouble spots so that you can fix problems and keep your network up and running a greater portion of the time. A seemingly small yet consistent uptime increase will pay off handsomely. Just imagine: your network is up just 1% more…day in, day out, that allows a couple more online orders a month to be entered from customers who otherwise wouldn't be able to buy from you…or when an idea strikes you at an odd hour, you can access files from home that wouldn't normally have been available at that time…

Example: You effectively use the network management tools that came with your firewall, and the result is your network is up 1% more every day. It doesn't seem like much, 1%. That's just 14 more minutes of uptime daily. If your average daily revenue is $7,700, typically made over 8 hours (or $16 revenue/minute), that means that extra 14 minutes should consistently bring in an average of $224 every day. At this rate, it won't take long to pay back the investment in the firewall …will it? And the network management features are also making your life easier.

5. Are Your Employees On Task?

One of the main sources of corporate inefficiency is inappropriate use of the Internet by employees during work hours. Repeatedly checking personal email, buying concert tickets, downloading music, surfing buy/sell sites, and other major time-wasters all sap your business' productivity. The solution isn't to turn all access to the Internet off. What needs to happen is that employees be allowed to visit certain sites that add value to your operation, and not be allowed to visit time-wasting Websites which have no connection to your firm. This is called content filtering.

A content filter is a useful feature often provided with a firewall product. It allows you to set up access level categories, say one for managers and another for employees, and parameters for filtering out unproductive Web content. Two ways have been developed for you to go about this (or you can use them together): a 'Ban List' or True Content Filtering.

A Ban List, or "Black List", is a specific register of sites deemed inappropriate (porn, gambling, email, music download sites etc.). It must be constantly updated as new sites pop up every day, which is expensive. To be banned, a site must be precisely included on the list.

True Content Filtering employs a set of algorithms and key words and phrases to search webpages the user wants to see *before* they see them. If the content matches the banned terms, then the site is blocked. This method is far more cost-effective and useful as it does not need attention by you after the initial setup.

Content filtering can be as restrictive or as free as you want it to be. Given the immense amount of corporate time wasted every day by inappropriate Internet surfing, though, it is certainly in your best interest to have some form of Web content filtering.

Example: Two of your employees are surfing the Web for music during work hours, and also hogging needed bandwidth by downloading song files (slowing the whole network down). Using features available with a good firewall product, you discover that in total they are wasting a half-hour a day. You engage the content filter feature and block music sites from being seen at the workplace. At $25 per hour pay rates, you have recovered $12.50 per day, or $250 per month of productive time. Also, you have increased the speed of your network by freeing up bandwidth (reports run faster, printers complete their jobs more rapidly, files load quicker), and that has a major positive spillover effect.

Web content filtering provides you an excellent return on investment, and keeps employees on task and safe on the Internet.

6. Are You Wasting Expensive Expert Time Updating a Ban List?

Having content filtering can make your business more productive; however, the tedious manual process of updating a ban list certainly is expensive. Especially if you're a small business owner who does not have a full time IT department—or only brings in an outside consultant when necessary—you *do not have* the resources to waste on the tiresome job of updating a ban list. When an IT person is in your shop, they should be working on important technical problems, not data entry! And *you* should not be doing this work, either.

Investing in a firewall product with a True Content Filter solves this problem. The block parameters are set up once, and then the filter runs automatically, only needing attention if there is a need for a 'tweak'.

Example: You notice the ban list update process takes 10 minutes a day three times a week for your $90 per hour IT consultant. That's $45 a week, or $2160 per year spent updating a list when the consultant should be spending that time and money doing more important things!
You immediately upgrade to a True content filter, ensuring the unnecessary job of manually updating a ban list is eliminated, and spend your IT budget funds more wisely.

A True (or Intelligent) content filter will inexpensively provide more flexible and effective protection for you and your employees on the Internet.

7. Are Your Business Processes Becoming Easier?

A very important feature packaged with good firewall products that businesspeople are looking for these days is called Virtual Private Network (VPN)/remote access. What VPN/remote access does is allows you to access your company data from anywhere, securely and quickly. This naturally is very useful in many business roles: say for example, for process improvement or management activities when you want to wander around the factory floor and have all the production data available on your wireless laptop; or your 'road warrior' salesperson wants to access client data from their hotel in

the evening to prepare a presentation. Encryption is a far more effective and strong level of protection than the slight level of username and password offered by other technologies.

Example: A sales visit to a big potential client in another city results in a Yes. There's just one hitch: the client has to see an example of a similar project you've done, together with all the technical files. In the past, this requirement would have delayed the signing of the contract by at least a day, as files were loaded to disk and couriered over. The sales meeting conclusion would have been on hold, and the team put up in the hotel for another expensive night. Now, the sales team can simply log in, download the project files, and impress your new client. Recalling the accounting dictum that "A dollar today is worth more than a dollar tomorrow," the financial returns from having VPN/remote access are plainly visible. The positive effects on your cashflow and productivity are virtually limitless!

Data sent and received over the VPN is encrypted to your firewall's protection level. Techs can remotely access your network if there is a problem—and nearly all the time, they can resolve issues without a costly site visit.

Example: A network problem is resolved by the consultant remotely logging in and fixing it. The time to solve the problem is 30 minutes. If the consultant had had to travel to your office, you would have been billed for an additional hour. At $90 per hour and an average of a problem a month, that adds up to well over $1000 by the end of a year!

VPN/remote access brings you many savings, coupled with the ability to be productive and use your data at non-standard locations and times.

Total all of the savings you realize from a good firewall product as listed in this report, and you'll find the firewall very likely pays for itself immediately.

If you agree that these seven measures are useful, why not use them to find out if your current IT investments are paying off?

For IT products that definitely pay off, call KDI at 1.800.661.1755 today!