Dealing With Information Technology

FOR EXECUTIVES

A Reference
for
All of Us!

NetSentron,
a division of KDI

404 - 17768 65A Avenue
Surrey, BC V3S 5N4
Canada

Call Us Toll Free: 1.800.661.1755

Great, Now
What do I do?

www.netsentron.com

Top 5 Steps for You to Successfully Deal With Information Technology:

1. **Have Experts Manage the Key Parts of Your IT Infrastructure, Not the Whole Network**
2. **Get an Internet Content Filter on the Job**
3. **Give You, Your Staff and Your IT Partners the Ability to Securely Work on Your Network from Anywhere**
4. **Make it Easy to Identify and Diagnose Problem Computers**
5. **Start Using an Auto Offsite Data Backup Service.**

Before we got on the scene, this is what the Information Technology (IT) situation was doing to a lot of our clients:

- Meetings were frustrating, argumentative affairs as departments and individuals tried to get support and funding for their pet 'magic bullet' IT solution
- The IT budget was an uncontrollable yo-yo from month to month, as unanticipated breakdowns made for costly fixes and deadly network downtime
- Frontline staff were annoyed because the computers were down so often they were constantly behind on work
- Corporate leaders were having trouble making good decisions, due to not having timely access to information.

Everyone would point their finger at everyone else, and IT repair costs soared as expensive emergency consultants were brought in to bring the network back to life. Nothing seemed to be getting any better, no matter how much money was dumped into the black hole of IT.

Any of this sounding familiar to you?

You've probably noticed a great deal of complacency in the world. People think and will tell you that they've got things covered, know what they're doing, have it all under control. No need to look at anything new, anything different. Well, if you want to get a different result out of your IT, you're going to have to look at something different. Let's look at **five things you can do** to control your IT costs and make computer frustrations disappear…

1. Have Experts Manage Only the Key Parts of Your IT Infrastructure, Not the Whole Network.

Other IT firms will typically offer you only two solutions: Break-Fix, or Managed Services.

Break-Fix is the most common way people handle their IT. Ignore the whole deal, then act surprised when something breaks, and shell out a pile of dough to fix it. There's the budget yo-yo. One month, no IT costs; next month, tens of thousands of dollars gone out of the blue.

Managed Services is the other option. Whole-hog, big dollars, "We'll handle everything down to the last mouse ball." Very expensive: $50 or more every month to watch a desktop PC. Well here's your first tip: Today, PCs are a commodity. You can replace one for around $400. There is NO need for you to be shelling out 1.5 times the value (or more) of the commodity every year to keep it running.

> **TIPS: Have one or two spare PCs on hand,** and for what you would likely spend in a *single month* of Managed Services desktop PC support, you'll be covered.
>
> **Also, have some basic in-house expertise.** Don't be calling expensive consultants for little problems, like how to do a mail merge or change a keyboard. Make sure your human resources include someone who can take care of mundane computer issues.

So what is there to help you beyond the 'yo-yo' of Break-Fix and the unnecessarily costly monthly expenditures of Managed Services?

Our recommendation is to protect your *core company data assets*—your server(s) and your network infrastructure. This will lower IT costs and ensure your infrastructure is kept up and running, and in our experience is what companies really need in terms of computer support. These are the expensive, less-easy-to-replace pieces of hardware that are the backbone of your IT. They enable you to process orders and keep the cash flowing, and access information quickly for timely decision making.

Internet — Firewall / VPN / Content Filter — Server — Desktop PC — Backup Device

In the above diagram, those things we recommend to be managed by outside experts are the firewall, server(s), backup device, and network connections (the red lines). This will result in you knowing with certainty what your monthly IT budget is going to be, and stop you from wasting money on paying consultants to manage commodities like PCs.

For more detailed information on such a program, visit www.kdi.ca or call us toll free at 1.800.661.1755.

2. Get an Internet Content Filter on the Job.

Many owners and managers don't think Website content filtering is important. To some degree, this makes sense: business needs to move forward, projects need to be completed, billings need to be sent out. Employee Web surfing seems to be a small issue, and content filtering unglamorous, not that necessary, and maybe even draconian. But hang on a minute: if you knew there was a process problem in your company that was leaking and losing you thousands of dollars a year, you'd jump and fix it at once, wouldn't you?

This is what the choice of not filtering Web content is doing to you and your company.

Schools caught on to this long ago. They like the NetSentron because of its combination of True intelligent content filter and traditional 'Ban List', which makes it very good at protecting students from inappropriate website content. School administrators use the NetSentron and its content filter because it stops people from seeing the wrong things on the Internet, and lets them see the right things.

Isn't that what should be happening when your employees use the Internet?

Without an Internet content filter, you are letting your employees waste time surfing for things that have nothing to do with your business. How much time and money is wasted?

- 30 - 40% of Internet use in the workplace is not related to business (IDC Research)
- Over 60% of all online purchases are made between 9AM and 5PM (Nielsens/NetRatings)
- 70% of all Internet porn traffic occurs during the 9-5 workday (SexTracker)
- 37% of workers say they surf the Web constantly while at work (Vault.com).

All this wasteful surfing adds up to a huge amount of lost work time that you are paying for! If a Web Content Filter recovered just 20 minutes a day that had been unproductive from <u>one</u> typical employee earning $20 per hour all-in, that would give you back $1,600 a year in productive work time. The content filter would pay for itself!

Get your free copy of the white paper
"Five Things You Must Know When Selecting a Content Filter"
and see further information at www.netsentron.com,
or call us toll free at 1.800.661.1755.

3. Give You, Your Staff and Your IT Partners the Ability to Securely Work on Your Network from Anywhere.

Many companies are allowing some employees to work from home. Others need to give access to "road warrior" salespersons, who may need to log in to the firm's network at a client's, or at a hotel. Unfortunately, most firms lack the technical expertise to really know how to create a secure network that remains accessible to the right people.

FACT: Username and Password is Insufficient Protection.

Company networks everywhere are lying around completely exposed. WiFi, for example, is not secure out of the box. You might use it at your operation and assume it's safe, but how many times you've heard someone say they've 'piggybacked' on someone else's signal so they don't have to pay for their home Internet connection? People often install their WiFi behind the firewall, believing it's secure…but think about it:

- You have a device *transmitting a signal out ranging from a few blocks to tens of kilometers or miles in radius*, protected by only a dinky, swiftly broken level of security—not the firewall's tough encryption
- WiFi devices are programmed to blindly let anything talk to them, meaning that anyone can deftly step past your firewall and get into your network that way
- Bots and programs are being run continuously by hackers and spammers to hijack your—anyone's—processors, which could very well result in you being blacklisted by your Internet Service Provider (ISP).

Not to beat up on WiFi only: employees can get your company computers hijacked and turned into 'zombies' simply by bad Internet browsing. "Click Here for Prize, you're our 100,000[th] customer!" and suddenly a spam application is silently installing itself in the background. In a little while, hundreds of thousands of spam emails will be sent from *your computer*, and the ISP will blame you.

You need network security experts to deal with these concerns. Your cousin who knows how to plug in a network card isn't going to cut it. This is a very important way to avoid disaster and save money by doing it right the first time.

Now more about saving money by taking advantage of Virtual Private Network (VPN) / remote access:

If you have secure VPN/remote access, nobody has to waste time trying to figure out what they need to download to their laptop anymore. With secure remote access, your people can bring the whole office with them.

If you've got multiple branch operations, data can be swiftly and safely sent across the Internet, making month-end reporting, inventory tracking, and decision making fast and timely. You'll get quicker access to information, and have a more agile company.

TIPS: **The best level of encryption** for remote access is by the largest key available, indicated by the "bit" number. Presently, the highest level of commercially available encryption is 256 bit. This is over one million times more secure than online banking! Look for a product with this encryption level. Breaking it is nearly impossible, and so time-consuming almost nobody would ever try.

Avoid user account fees. Most VPN/remote access providers will charge you an account fee for every person you need to set up a connection for. Make sure you choose a supplier that doesn't do this. Rather than spending a ton of money every month on remote access accounts, get a device that allows you to set up as many as you need at no extra charge.

Consider using a security certificate. This is an additional layer of safety that you can use along with encryption. The certificate proves you are who you say you are. You might not need this level of security all the time, but having a product which allows you to make use of it is advantageous.

With VPN/remote access, you will also save big dollars on consultant fees, because nearly everything an IT guy will have to do to help your network can be done over the Internet. The tech will not have to charge you for expensive and wasteful time spent traveling to and from your office. Issues will be resolved more quickly and cheaply.

To learn how to choose a firewall, and see one that includes virtually unlimited VPN/remote access connections, visit www.netsentron.com or call us toll free at 1.800.661.1755.

Secure VPN/remote access example:

Remote Access User
(Eg. "Road Warrior"
Salesperson at Hotel)

Firewall / VPN /
Content Filter

Server
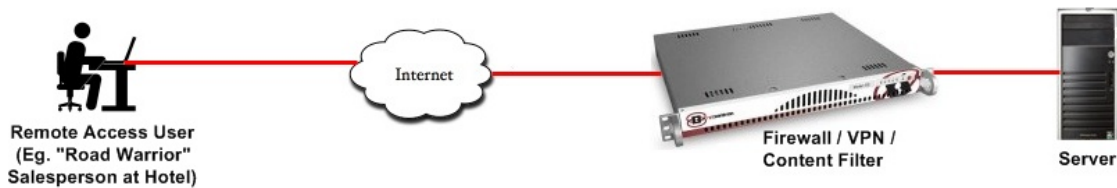
4. Make it Easy to Identify and Diagnose Problem Computers.

Scenario: The whole system is bogged down, running at a snail's pace. Staff are freaking out because they can't do their work. Frustration levels are at an all-time high.

Half the employees have no idea what's going on, and the other half are shouting that you have to upgrade your computer network, *yesterday*. You, meanwhile, are cursing the day you approved moving the company's order entry, inventory tracking and purchasing functions "onto the Web" through that new application.

Ever had a day like this?

Truth is, it might not be your network infrastructure that's the problem. What might really be happening is that one desktop computer is hogging the firm's Internet bandwidth, because Joe the Stock Guy got bored and is downloading his favorite tunes.

But how the heck are you ever going to find that out, and avoid dumping tens of thousands of dollars into a completely unneeded network upgrade?

Solution: Traffic Shaping & Bandwidth Monitoring tools (and a Web Content Filter would sure help, as discussed above).
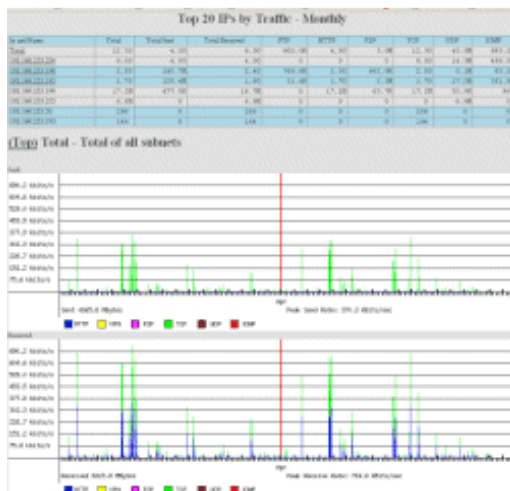
With bandwidth monitoring tools, you can rapidly identify which PCs are having the most traffic with the Internet. If there's a virus, you can pin down which computer it's on. If somebody's streaming movies onto their desktop, you'll see that too.

Then, you can stop them from doing that, either by blocking the sites with a content filter, or by throttling the bandwidth individuals can use by traffic shaping. These tools give you simple-to-understand graphics to solve network problems with.

5. Start Using an Auto Offsite Data Backup Service.

If you don't have some kind of file backup system in place, you are dancing with disaster.

"Fifty percent of companies that lose their data go out of business immediately and ninety percent don't survive more than two years."
~Baroudi Bloor International

The *National Computer Security Association* says that without adequate backup it takes:

- **19 days and $17,000** to recreate just 20 MB of lost **sales/marketing data**
- **21 days and $19,000** to recreate just 20 MB of lost **accounting data**
- **42 days and $98,000** to recreate just 20 MB of lost **engineering data**.

20 MB isn't very much data. As you can see, the costs of not having secure offsite data backup mount into the tens of thousands of dollars, just in recovery. This doesn't count the lost income while you try to put everything back together. You can see how most businesses just don't survive after experiencing significant file loss.

Some businesses back their data up on a tape. Here are two problems with that method:

1. The eventual failure rate of all backup tapes is 100%
2. Backup media left in your office have little value, because they'll likely be destroyed in the same disaster that takes out the rest of the place.

The most effective insurance you can get to ensure your business can quickly recover and survive after a disaster is offsite data backup.

An automated service that backs up your data every night to a secure, offsite location is the best way to protect your business. If something terrible happens, like the receptionist's PC dies or a flood wrecks your server room, all you have to do is easily recover your data from the offsite storage and you're back in business.

To see an example of an automatic offsite data backup system and learn how it insures your business, visit www.netsentron.com or call us toll free at 1.800.661.1755.

Let's sum up 'Dealing With Information Technology for Executives':

1. **Have Experts Manage the Key Parts of Your IT Infrastructure, Not the Whole Network. Use In-House People to Take Care of Day-to-Day Issues**
2. **Get an Internet Content Filter on the Job**
3. **Give You, Your Staff and Your IT Partners the Ability to Securely Work on Your Network from Anywhere**
4. **Make it Easy to Identify and Diagnose Problem Computers**
5. **Start Using an Auto Offsite Data Backup Service**

Acting on these five points will help you have:

- Productive, functional and friendly meetings, with everybody on the same page regarding the computer network
- A controlled, lowered and stable monthly IT budget
- Staff who are contentedly able to do their jobs in a focused manner because the network is running smoothly, and bad websites are filtered from view
- Timely access to information, so your corporate leaders can make better decisions
- The ability to be productive at times you previously could not have, with complete access to your data
- Fast resolution of computer problems, and increased network uptime
- A protected business that can quickly and straightforwardly recover its data and get back into operation even after a disaster.

But don't take just our word for it…

A Quick Case Study in NetSentron-Generated Savings

"Investing in NetSentron not only provided our offices in Edmonton, Alberta and Delta, BC with very secure over-the-Internet network connections: it also paid for itself and saved me over $70,000 in 'hard costs', and much more in 'soft costs', over five years. NetSentron made all kinds of business processes faster, and that helped our people instantly become more productive."

Linda Simpson
President, Western Concord

Linda needed two of the larger NetSentron models and upgraded from the frame relay infrastructure her company had been using. The upgrade totaled about $7,000. Linda's investment in NetSentron was paid back in six months, and she continues to save over $10 over the past five years for every $1 she invests!

We're glad to answer any of your questions about how to save you money on network security and support. **Unlike other IT firms, we don't prescribe the solution before we've seen the client.** Call us at 1.800.661.1755 to discuss your specific situation.

www.kdi.ca ● www.netsentron.com

NetSentron

A Division of Kobelt Development Inc.
#404 – 17768 65A Avenue
Surrey, BC V3S 5N4
Canada

Toll Free: 1.800.661.1755
Local: 604.574.7225
Fax: 604.574.7256

www.netsentron.com
www.kdi.ca