A TRS Technology Solutions Guide To Small Business Network Security!

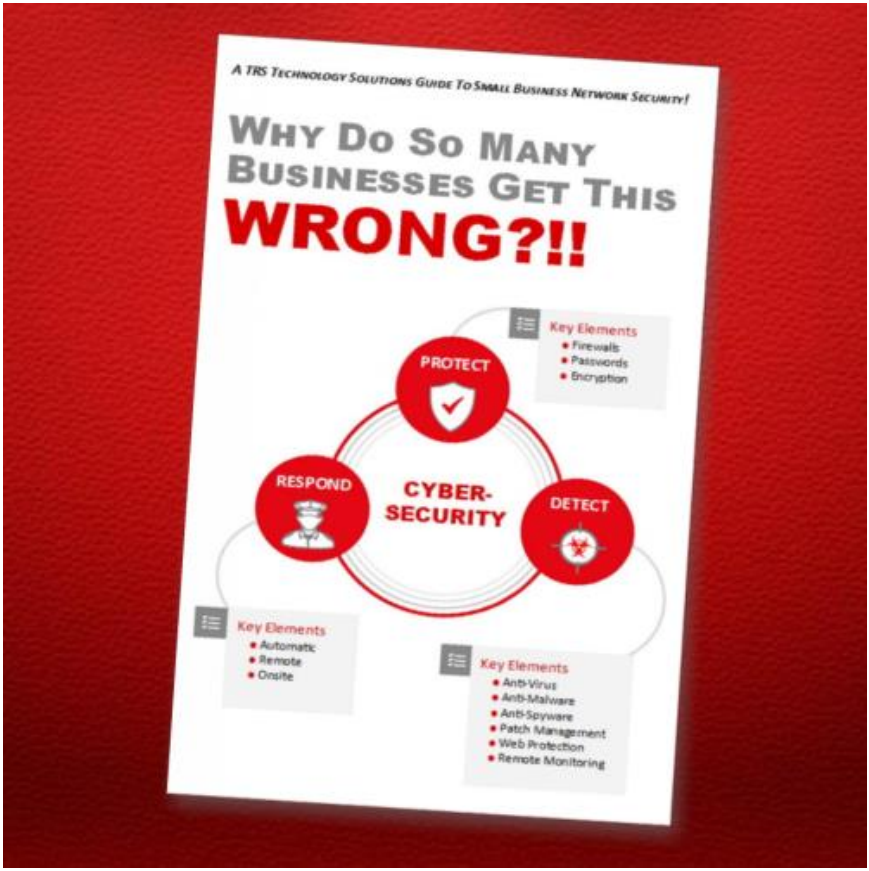
CORE 6+

BUSINESS NETWORK SECURITY PLUS

SYSTEMIZED, REAL-TIME BUSINESS CYBER-SECURITY

The Network Security Every Small Business NEEDS TODAY!!

Before you start this book, it is my hopes that you would have already finished my previous book:



While this book is a *DEFINITE MUST READ* for any small business or nonprofit decision maker, it is somewhat of a supplement to the previous book (*shown above*).

This one picks up on and expands concepts presented in the previous book. If you don't have it, please visit:

http://trsets.com/cs-pdr/

Please Let Me Remind You Why This Is So Important…
THESE ARE REAL NUMBERS, *THAT SHOULD SCARE YOU!*

THESE NUMBERS WERE MOST RECENTLY UPDATED OCTOBER 27, 2020

You can Google these numbers yourself, and you will find:
"At least one-third (over 32%) of all computers in the U.S. are infected with some form of malware."

The Wall Street Journal reports:
"Over 250,000 computers are affected by malware every day…"

You may be horrified by the fact:
"Over 350,000 new malicious programs, malware and other unwanted applications are created every day."

SonicWall stated:
"There were 9.9 Billion malware attacks reported in 2019."

The cost of malware has skyrocketed:
"In 2015, the global cost of malware was an already staggering $500 Billion USD. Now that number has grown four-fold, with the annual economic toll of cyber-crime in 2019 reaching over $2 Trillion USD."

FBI statistics show:
"The average malware lies dormant for about 250 days before being used against the company."

FBI also says:
"The average time for a company to detect an actual malware attack is about 14 months."

The Scariest Stat of Them All:
"EVERY MINUTE, AT LEAST FOUR COMPANIES FALL VICTIM TO A RANSOMWARE ATTACK."

Those are some very disturbing and eye-opening numbers. The Internet knows no boundaries. Every one of us – *personally and professionally* – and all of our computers, laptops, tablets and smartphones are at risk.

Before I go on, let me remind you:

> ***Malware*** *is software with Malicious Intent.*
>
> ***Ransomware*** *is a Malware that hijacks all your data and then threatens to "Delete Your Files" if you do not pay the Ransom.*

Here's the best way to think about Malware…

If your computer has Malware on it, this means that:
Someone From Outside Your Company, Someone You Do Not Know, has installed some software on your computer. Now, they potentially have access to all of your files, all of your data, all of your keystrokes, all of your logins, and ***YES!*** this even includes all of your personal and commercial bank and investment accounts.

Many forms of malware can also hear your conversations through your PC-Mic, and/or even see you through your computer's WebCam.

How does that make you feel? *Concerned (I hope)… maybe even sick…*

As I said above, the Internet knows no boundaries, and in today's digital world, basically everything we do is online, including: Family; Friends, Photos; Entertainment; Banking; Shopping; Coffee Orders; Food Orders; Car Rides; Etc. Social Media has replaced in-person engagement:

> *People share their lives on Facebook and Instagram. They opt for texting over phone calls. They "hangout together" in chatrooms rather than at coffee shops and friends' houses.*

If you're in business, there's a good chance that at least half of your applications are already in the Cloud. Your Suppliers are connected. Your Customers are connected. And with this pandemic, and the "New Normal," I'm betting now, even your employees have to be connected.

THE TREND IS UNSTOPPABLE.

With everything being online – meaning everything is accessible from ***literally*** anywhere and by anyone who has Internet – allowing the ***right*** people to have access while keeping the ***wrong*** people out is becoming increasingly difficult. The Security Equation Has Changed…

AND IT'S ONLY GOING TO GET WORSE.

In a recent study, the 9/11 Security Commission stated:
"Our most pressing problems are the daily cyber-attacks against our nation's public and private networks."

Ransomware is so prolific, and seemingly unstoppable, that Hackers are actually setting up "Customer Service" Call Centers and Websites to help their clients – ***I mean victims*** – walk-through the payment process. This even includes having Live Operators working the phones so the victims can call in and get clarification on payment options – with some even negotiating a lower ransom.

Do you understand what that means?! These attacks are so profitable and such a common occurrence, and knowing they can't be stopped, Hackers are building "Customer Relationship" services for their victims.

I know since you're reading this, you're probably a Small (or Very Small) Business Owner or Leader… and you're already thinking to yourself: ***"My business is too small. No one is trying to hack into my business."***

BUT THAT'S JUST NOT THE CASE!

THE TRUTH IS: NO BUSINESS OR INDIVIDUAL IS SAFE!

And the reality is: Small Businesses are often the primary target of cyber-attacks, simply because they are easy prey. ***And let me be clear:*** Small Businesses are not individually "*directly targeted.*" It's more about the fact that Small Businesses seldom invest in adequate Cyber-Security, which leaves them vulnerable, susceptible and exposed as easy targets.

There are certainly skilled cyber-criminals (*the world-over*) who will take the time to plan and perpetrate multi-staged, sophisticated attacks on a specific organization (*for all sorts of reasons*). But…

The Majority of Attacks Against Small Businesses Are Not Targeted. Even Worse, They're Not Even All That Sophisticated.

Small Businesses often become victims of petty, unsophisticated and rudimentary attacks, simply because they do not have even just the simplest aspects of cyber-security and network protection in place.

WHICH IS WHAT THIS BOOK IS ALL ABOUT!

There are three main reasons for a lack of investment in cyber-security:

(1) **Simple, Honest Unawareness…**
Most small business owners and leaders simply do not understand how real the threat is and don't even know what basic network security elements they need.

(2) **An Uninformed, False Sense of Security…**
There are those out there, that for any number of reasons, just don't believe it can happen to them. They think their business is too small, and that no cyber-criminal would ever take the time to attack them. Saying things like: "*That kinda stuff only happens to other people, not l'il ol' me…*" Not taking to time to realize that to the other 7.8 Billion people on this planet, they are the other person.

(3) **Perceived as Too Expensive, and Not Worth It…**
Which I can understand. Especially as I learn more about what all these "Other Guys" are charging. Some of these other options are *awfully expensive*. It's even worse when you combine these other high-priced protection options with a false sense of security. If you don't think you're at risk to begin with, of course it wouldn't make sense to spend so much money on services you don't think you need.

It is my goal – ***Actually It's My Mission*** – to help Small Businesses and Nonprofits, *just like yours*, better protect themselves, their employees and their clients from today's cyber-criminals**…**

WITH A POWERFUL SOLUTION ANY BUSINESS CAN EASILY AFFORD!

I have – ***literally*** – invested the last three-plus years of my life creating, testing, validating, and improving ***The Absolutely, Most Cost-Effective Cyber-Security Solution for Small Businesses and Nonprofits***:

The **Core6+** solution is a ***Layered Security Platform*** that delivers the most comprehensive network security solution available. Giving you the best proactive, detective, and reactive solution available today.

LET ME SAY THIS AS CLEARLY AND CONCISELY AS POSSIBLE:
THE VERY REAL TRUTH IS: WE CANNOT STOP HACKERS!

Hackers' and their ploys are becoming more and more sophisticated. Hackers' tools are becoming more formidable and powerful every day. Social Engineering tactics with a purposeful approach can always get in.

Continuing forward in this Digital Age, means new technology and more automation every day, which also means more vulnerabilities every day.

We Cannot Stop Hackers. We can only get better at detecting and responding, and hopefully stopping the attacks before it's too late.

Which Is Exactly What The Core6+ Platform Does!

There are six core security components associated with any and every network, regardless of size. Home Networks, Small Business Networks, even Enterprise-level Global Networks, all require the same protection.

These six core components are:

(1) Gateway Protection
(2) Wireless Protection
(3) Anti-Virus/Anti-Malware
(4) Software Updates
(5) Web Protection
(6) Data Protection

If your organization is missing appropriate ***up-to-date*** coverage with Protection, Detection and ***Real-Time*** Response-enabled tools in any of these core areas of network security, then your organization is easily susceptible to even some of the most elementary of cyber-attacks. ***There is a high likelihood you already have malware on your systems.***

THERE IS NO OTHER WAY TO SAY IT:
If you have not already deployed a Detection and Response focused Security System, like Core6+, your likelihood is 100%.

It's an almost certainty it's already happened. Remember the stat from before? ***One in Three (30+%) of U.S. computers are already infected.*** How many computers does your business have?

Is your organization's network secure? If you are a Small Business or a Small Nonprofit, then in most cases, probably not.

It's Always What You Don't Know
You Don't Know
That Costs You The Most…

And you don't know – ***for sure*** – if your organization's network is safe.

You cannot just look around and pretend since you don't see anything wrong, and no one is complaining, that everything is OK. When you do that, you're risking everything you've built and worked for to this point.

It is my mission to help small organizations, *just like yours*, move from zero and/or minimal protection to adequate and/or hopefully better than just "good enough" network security.

The **Core6+** solution consists of a layered and balanced security architecture. One that offers an appropriate level of Protection with specialized tools to provide early Detection, and Real-Time Response that can counteract an attack before it's too late.

Cyber-Security is ***NOT*** just some out-of-the-box product you can buy, install and then now you're safe.

Cyber-Security Is A System… With A Definitive Process.

The **Core6+** solution is an investment in Systemized, and Real-Time Cyber-Security Protection, Detection and Response.

It's designed specifically to help you minimize your overall risk, maintain a low risk threshold, and includes tools for Early-Detection, Immediate Alerts and can even provide Real-Time Response… ***Before It's Too Late.***

I am dedicated to Nonprofits and Small Businesses, who I truly believe have been historically underserved and/or overcharged when it comes to Technology and Managed Services. ***I'm doing everything I can to make Cyber-Security EASILY AFFORDABLE and EASILY IMPLEMENTED.***

I know the system I have built is BY FAR the most cost-effective solution available to help small businesses mitigate risks, stop most threats, and detect and respond to infected computers, unauthorized users, and intruders with malicious intent, BEFORE they reach your data.

UNLIKE EVERY OTHER (ALMOST) SIMILAR SMALL BUSINESS CYBER-SECURITY OPTION OUT THERE…

With my system:

You Only Pay For The Services You're <u>Actually</u> Getting!

It's not – ***AT ALL*** – based on a high, per device or per user fee, that is *somehow* supposed to include some level of "additional" service.

It is my position, that way too many Managed Service Providers (MSPs) use the "Free" or "Included" or "Unlimited" Helpdesk offer as a ruse to simply bill you more money per device or per user.

It is my position, that if your network was clean and secure most Small Businesses and Nonprofits would have very little need for "unlimited" Helpdesk support… *at all*.

It is my position, that way too many MSPs grossly over-charge Small Businesses and Nonprofits for applications and services provided.

Again, this is just ***my position***… and let me be perfectly clear: I'm not saying ***all*** MSPs are taking advantage of you… I said "***way too many***…"

The worst part is, it's not really these other MSPs fault, not directly.

Trying to find ways to bill clients more while actually providing and doing less is a Managed Services Industry Standard.

I cannot even begin to guess how many (hundreds of) books and articles and training sessions I've encountered over these last few years that specifically strategize how to make more money per client while actually doing less work… and let me "*let the cat out of the bag*:"

The First, Most-Common MSP Profit Strategy: Just Charge More

Now, I'm certainly in business to make money… and I'm all for making a better-than decent living, but not at the expense of my moral compass – and certainly not at the expense of another Small Business Owner or a Nonprofit who is serving the community by ***literally*** doing God's work.

These Managed Services Industry "Play Books" will tell you – in very simple English – if you want to make more money as an MSP, the first best thing you can do is simply raise your rates… *across the board*.

> "Charge more per device/user per month."
>
> "Charge more per hour for additional services."
>
> "Increase your onsite visits to a Two Hour Minimum."
>
> Etc. Etc.

For some reason, these other MSPs believe that by simply raising their rates you will believe they provide a better service… after all, look at how much they cost… they have to be doing something "good" for all of that money… right?

Wrong. Unfortunately, the answer is No. They really are just taking advantage of human nature's perception that price equals performance: "*The more you pay, the better you get.*"

Which I know is true in certain aspects, especially where there is a true, tangible benefit associated with the additional fees. But in the case of most MSP offers, the only benefit – *for anyone involved* – is that the MSP now has a larger margin of profit for their own bottom line. There is no real, tangible benefit for you associated with their extra fees.

The upsetting thing (to me) is "Just Raise Your Rates" is straight out of the Industry Playbook… just like" "Make Sure You Get Your Overages."

MSPs are always looking for new ways to create and/or increase "overages" – which is the money they charge you over-and-above any monthly recurring fee.

One of my most ***unfavorite*** ways MSPs are told to "cash in" is to simply:

> "Increase their onsite visits to a Two Hour Minimum."

And again, I'm not saying ***ALL*** MSPs are taking advantage of you… I'm just saying these tactics to increase revenue while actually doing no more work are right out of the Managed Services Industry Playbook.

Obviously – *in case you can't tell* – Managed Services has almost always had a negative stigma in my mind.

Maybe it's because I've been able to see so much "behind the curtain" at the business model, and have heard so many stories, ***first hand***, how the "successful" MSPs make their money (*by simply just Over-Charging*).

And I must say:

I AM NOT A FAN OF THE TRADITIONAL MSP REVENUE MODEL!

WHICH IS EXACTLY WHY I'VE CREATED MY OWN HYBRID MANAGED SERVICES OFFER.

I'll show you just how perfect it is (***and just how much money it will save your organization***) in just a minute, but first I want to make sure you understand what the traditional Managed Services offers usually are...

You would think—*and for the most part it is true*—that the MSP business model is all about helping businesses manage their IT needs, that's computer and networking, including CyberSecurity, and the overall costs, thereof.

And again, *for the most part*, that is the goal of most MSPs.

Where usually the only differences between the different MSPs and their specific offers, is not so much in the services they provide, but in the prices they charge for those services.

Certainly, some MSPs have preferred/niche experience with certain businesses and or industries. Maybe even certifications in industry-specific software or platforms. Maybe even years of experience with a certain industry's rules and regulations.

But beyond a specific, industry-related certification, almost all MSP offers are the same.

At the preferred level, they almost always provide:

- Managed Anti-Virus/Anti-Malware
- Managed Patches and Security Updates
- Managed Document/Data Backup
- Managed Firewall and Content Filtering
- Managed Web and User Protection
- Remote Device Monitoring and Management
- Over-the-Phone Helpdesk Service
- Etc., etc.

With minimal variations in the Service Level Agreements (SLAs).

Some will include all-inclusive Over-the-Phone Helpdesk Services; some will limit this to a fixed time allotment, like a Maximum of 15 Minutes (or so) per Covered Device Per Month; others simply state Two Hours (or Three, or Four Hours) of Free Helpdesk per month; most actually include "Unlimited" Helpdesk Support during Normal Business Hours.

Some might – *most rarely do* – include some version of a fixed time allotment for Onsite Support (like a Monthly Block of Hours) as well.

Some might include Daily, Weekly and/or Monthly Reporting.

Most will include a Quarterly Business Review, so they can schedule time to sit down with you and tell you everything they've done over the last quarter, and you can tell them about new projects or changes that are coming up in the next quarter.

As I've said, almost all of these services are the same. And do you know why? It's because, as an MSP, there are only a handful of actual service platforms we can choose from to deliver these services.

At my last count, there were 11 ***reliable*** Managed Services Platforms.

This means, across the globe, all of the MSPs have to choose from these exact same platforms to service and protect our clients. And because all of these platforms have very similar pricing, we MSPs basically all pay the same thing to protect, monitor and serve each computer.

Which, now, should certainly highlight the largest variance in MSP offerings, which is the pricing models and revenue strategies.

This is where the majority of the other MSPs lose my agreement in the way they do business.

As I've already alluded to, the MSP Business Model is ***notoriously*** based on (what I refer to as) the "MAILBOX MONEY" concept, which is then further surplussed and subsidized with the industry "OVERAGES."

As I've already stated: of course, I believe that if you're in business, you're in business to make money…

What I don't believe, is that you should have to take advantage (directly, or indirectly) of the people and/or their businesses to do so…

WHICH IS THE BIGGEST DISCONNECT FOR ME.

The Standard Managed Services business model looks like this:

1) Provide a Set of Managed Services
   (*like the list on the previous page*)

2) Charge a Flat-Per-Device (or Per User) Fee Per Month, for the services.

3) Find ways to bill the client more money each month so you can stack-up your "Overages" – like Onsite Service Calls, or additional "not included" services.

Which, on the surface, makes sense. Again, no one goes into business to ***not*** make money. But where these "Other Guys" and my way of thinking start to differ, is this:

If I'm Already Paying You A Hefty Fee (Per Device/User), As My Flat-Rate, Monthly Managed Services Charge…

Why Am I Still Having To Pay For All Of These Other Issues?

Look, I know problems will arise. I know accidents happen. I know, every once in a while, things are going to break. I know, at certain times, things will require additional attention.

My problem is when it seems like "every once in a while" is actually EVERY MONTH!

To "protect the innocent" – *and actually all involved* – I'm going to tell you a **REAL** story, presenting true facts and figures. I'm just not going to mention the names of those involved.

There is a small Nonprofit organization—in Central Texas—that has subscribed to a local businesses' Managed Services offering.

This "Example" (*BUT VERY REAL*) Nonprofit is currently paying $55 per computer, per month for the basic (*meaning the *NOT* All-Inclusive*) Managed Services Plan.

This Nonprofit currently has 18 computers, and a Server, which is $120 per month for the Basic Server Managed Service Plan.

So let's do the math:

18 Computers x $55 each = $990.00 per month...
1 Server x $120 each = $120 per month...

That's a combined total of $1,110 per month…

This $1,110.00 per month does include *ALL* Over-the-Phone Helpdesk Support – during Normal Business Hours (M-F/8-5)… Which the Nonprofit rarely uses, except *basically* every other Wednesday.

You see, *basically*, every other Tuesday night, the MSP runs the updates to the computers and servers remotely, and almost without fail, there will be a problem that the Nonprofit has to call support about.

Often times, these problems (*supposedly*) cannot be fixed remotely, and an MSP Tech will be dispatched onsite to work through the issue, and/or roll-back the update. Which is fine, right?

Well… Not Really…

The Basic Plan, offered by the MSP does ***NOT*** include Onsite Visits, thus the Nonprofit is billed a TWO-HOUR-MINIMUM – ***YES! You Read That Correctly: A TWO HOUR MINIMUM!*** (*Right Out Of The Playbook*) – for the MSP's Tech to show up a fix a problem they basically created.

With an Hourly Onsite Rate of $125.00 Per Hour, plus a $25.00 Flat-Rate Trip Charge to get to the Nonprofit's facility, often times this Nonprofit will end up spending $275.00 for the MSP's Tech to be onsite for less than an hour.

Keep in mind… This happens almost every other Wednesday.

So now let's look at the numbers:
The Nonprofit pays the "Base Fee" of $1,110.00 every month, but quite often pays $1,385.00, and sometimes $1,660.00.

Sometimes they pay $1,935.00 and at least twice a year they pay over $2,200.00 for just one month of support on less than 20 machines.

I wish I could say this wasn't a common practice.

I wish I could say that this type of service delivery and revenue "forcing" was limited to one certain local MSP.

But the unfortunate reality is that this type of "Overages" billing situation is right out of the Industry Playbook. This is a very common and Standard Revenue Model for MSPs, the world over.

What actually separates this provider from a lot of the others, is that they only charge $55 per computer per month… instead of $65, or $85, or even over $100 per month, per device/user.

Here's something else I want you to remember. The differences in rates have very little to do with the actual services performed and/or the technology delivered.

For the most part, there are only a few truly respectable MSP Platforms, known as IT Service Management (ITSM) Platforms. This is where we get the Managed Services applications—like the Managed AntiVirus, the Web Protection, the Patch Management, the Backup, etc.

And again, they are all fairly consistent in application functionality, service deliverables and ***most importantly***, pricing.

Which really means, the actual biggest difference regarding your per computer, or per user, price is directly related to the MSP's Overhead and (*pardon my directness:*) Greed.

It should be obvious, but if your MSP has offices in some high-rise, fancy-schmancy facility with parking garages and catered lunches, you're certainly going to pay a premium, just to cover their own costs, not because they provide a better service.

And/or, if the owner of the MSP has a "Silver Spoon" mentality and only wants the "finer" things in life, like fancy suits and Rolex watches, then you're going to have to pay more, just so they can make more and keep up with the luxurious habits of the owner.

Again, I want to reiterate, I have no problem with people building a business and making however much money they want to make, *for whatever reason*… But what I also know is:

Those types of Managed Services Pricing Models don't fit well within the Local Central Texas Small Business and Nonprofit marketplace.

Let's let those MSPs work for the banks and other financial services; or maybe some of the Personal Injury law offices around town; or any other industries where the value of the dollar is, *shall we say*, a little more loose.

Here's What I Want You To Consider:
How much more good do you think our Example Nonprofit could do each month if they were able to save even just 25% of the money they spent on Managed Services and the Overages?

What could your Nonprofit do with an extra $8,800 this year?

That's right… $8,800.00 is easily how much the Overages and even just a 25% discount would have saved our Example Nonprofit in the last year… and in reality, they could've been saving this $8,800 for the last six years!

OK… So I know your "wheels are turning" and you're trying to make sense of this. I know some of you must be asking yourself, do they have to pay $55 per computer. Aren't there other Managed Service Providers out there?

Well, of course there are. Some charge more. Some have bad reputations. Some, because of their own pricing model (***and their own moral compass***), opt to not do business with small Nonprofits, because they already know their pricing structure is not a good fit…

But, as I say all of the time:

It's Always What You Don't Know
YOU DON'T KNOW
That Costs You The Most.

And almost no one (YET) knows about our amazing Managed Services Offer designed specifically for Small Businesses and Nonprofits…

BUT YOU'RE ABOUT TO…

Let's look at the facts:
Our Example Nonprofit knows they need to make sure their computers and network are protected, monitored and managed. They also know enough to know they needed professional help to make sure this was done correctly.

So we have to applaud their awareness… and the fact that they took action to find a provider that (*at the time*) was the best fit for their organization and budget.

When we break it all down, the only real problem is, MSPs are not designing their businesses and revenue models for Small Business and Nonprofit clients. Which means, Small Businesses and Nonprofits, just have to succumb to the MSP's pricing model if they want Managed Services.

UNTIL NOW… ENTER TRS!

I *have literally* spent the last three-plus years building, modifying, testing and perfecting my own Hybrid Managed Services Offering... *SPECIFICALLY DESIGNED FOR SMALL BUSINESSES AND NONPROFITS!*

AND…

IT IS NOT BUILT ON THE MAILBOX MONEY REVENUE MODEL—AT ALL!

IT IS SPECIFICALLY DESIGNED SO YOU ONLY PAY FOR THE SERVICES YOU ARE ACTUALLY GETTING!

Can you even imagine?

What a crazy idea?

Only pay for the services you're actually getting?

What kind of wild-haired scheme is this?

Well, simply stated:

It's the kind of plan I would want for my own business.

Think about it this way:
The Standard Managed Services Plans and Revenue Models are designed so that you pay a flat, monthly fee for whatever included services your plan offers. Which is fine… BUT…

Then, the MSPs seemingly always find a way to bill you more, every month… Even though, you were sold on the concept that the flat, monthly fee would provide you a consistent amount and allow you to budget for your network support expenses.

Let's take this piece of the conversation to the next level…

Ask Yourself This Question:

If you are already paying a flat, monthly fee to maintain your computers, shouldn't your computers be having less and less problems… NOT More and More?

I definitely understand any upfront costs for device and network "normalization" and system optimization (also known as "Onboarding"), as well as security and performance enhancements… BUT… Once you work through all of my problems, shouldn't my computers and network be fairly consistent—AND MUCH MORE EASILY MANAGEABLE?

Shouldn't it actually cost me less each month?

What I'm saying is – in my perspective – the MSP (at least over the first few months) should have already worked through all of my computer's problems and got my network into a "clean" and manageable state.

Meaning, there should be less and less problems to fix each month.

Why would I always be charged SO MUCH PER DEVICE EACH MONTH, and then still suffer all of the additional costs for "Overages?"

Does that make any sense to you?

It doesn't make sense to me…

If you tell me you're "managing" my computers and network, yet there are ***always*** problems… I just don't know if I understand – or can even trust – your "management" skills.

It makes me wonder– *to some extent* – if the MSP is actually causing the problems *on purpose (or not)*, like in the case of our Example Nonprofit?

Before I get too far off on that tangent, let me just say this:

The industry standard "game plan" for Managed Services is very similar to Vegas:

The house (MSP) always wins…
and for the most part, we always
spend more than we ever intended.

SO… THAT'S WHY I CREATED THE PERFECT SOLUTION...
WHERE YOU ONLY PAY FOR WHAT YOU ACTUALLY GET!

The previous pages, you've just read to get you here, are now all going to be well worth the read.

I can tell you, for sure, across Central Texas, that's Waco to Georgetown, and Bryan/College Station to Burnet/Marble Falls, you will find less than 25 "true" Managed Services Providers.

Their per device monthly fee ranges from $27 for basic services to over $140 (per device/per month) for the more "all-inclusive" services.

With that said, all of the "bigger players" average about $60 per device per month for the Normal Business Hours Helpdesk service level. There is one (that I know of) that actually includes two hours onsite per month, as well (as long as you have more than 10 computers).

Every one of the lower-priced plans, have additional charges for the Offsite, Full-Scale Backup Solutions, as would be needed for a Business Continuity and Disaster Recovery (BCDR) plan.

Also, each of these have Server prices of at least $75 per month, up to $325 per month—depending on size, role and scope of the server as well as the associated and included Managed Services.

So, using these average pricing models—let's just, for example pricing-sake, say we use $50 per computer and $125 per server—and pretending that you only have 15 computers and one server, you would be paying $875.00 per month for basic coverage.

Let's also not forget there could possibly be a couple of hundred dollars (or more) each month in "Overages."

Meaning you could easily be paying over $1,000.00 per month, every month, for 15 computers and a server… That's over $12,000 per year…

Now check this out… and… I guess, first let me make sure…

Are you sitting down?

I don't want my numbers to "knock you off your feet"…

BUT… This is very exciting…

ESPECIALLY IF YOU ARE A NONPROFIT!

With the TRS Proprietary, Hybrid Managed Services Platform… You get, what we refer to as the Base 4+, that's:

Core 3 - Managed Anti-Virus/Anti-Malware
Core 4 - Managed Web Protection and Content Filtering
Core 5 - Managed Patches and Security Updates
Core 6 - Managed Basic Document Backup
+ Remote Automated Device Monitoring
+ Remote Device Management

+ Remote Device Access and Control
+ Asset, Software and Hardware Tracking and Reporting
+ Virtual CIO/CTO with Scheduled Quarterly Business Reviews
+ End-User Cyber-Security Awareness Training
+ Daily, Weekly, Monthly and Quarterly Reporting

ALL FOR ONLY $16.00 PER COMPUTER FOR A STANDARD BUSINESS

Only $8.00 Per Computer For A Nonprofit!

AND ONLY $75/$45 (RESPECTIVELY) PER SERVER, PER MONTH!

With regards to Helpdesk and Remote or Over-the-Phone Support, you do have to pay for any and all service, but only at an $85 per hour, broken down into 6-Minute increments (or .1 Hours)…

Meaning, if we do have to help you with something, and it only takes 10 minutes, we are going to bill you .2 Hours at the $85 rate, or $17…

BUT… AND AGAIN: ***ARE YOU STILL SITTING DOWN?***

As a Nonprofit, TRS, through the 501C3 Technology Initiative is going to discount that rate by 25%... So now, your $17 only costs $12.75.

So let's compare the TRS rates to the example on the previous page...

Let's say you are a standard Small Business and have 15 Computers at $16.00 each per month, that's only $240 per month, *NOT* 15 times $50 each, or $750… Plus, you save an additional $50 on the Server.

That means you immediately save $560, which translates to 64%!

As a Nonprofit with 15 Computers at $8.00 each per month, that's only $120 per month, *NOT* 15 times $50 each, or $750… Plus, you save an additional $80 on the Server.

That means Nonprofits Save $710, which translates to 81%!

With regards to onsite support, we will bill you the $85 per hour (or $125—depending on the support level required) plus any applicable trip charge.

But, since you're on our Managed Services Plan, **you will have a 30-Minute Minimum**, not one hour (or two hours) like the "Other Guys.

Plus, if you're a Nonprofit, you will also get a 25% Discount on these services as well.

So not only will we save you up to (and possibly over) 80% every month on the Base Fees, we will also save you 100's if not 1000s of dollars every month on "Overages."

It should be very easy for you to see just how powerful the TRS Hybrid Managed Services Offering really is and can easily project (or at least guess-timate) just how much money the TRS Managed Services Offer will save your organization while creating, securing and maintaining your Small Business or Nonprofit's network and computers.

And… just in case you forgot, or didn't quite catch it earlier:

The actual services provided by TRS to your Nonprofit, the AntiVirus, AntiMalware, the Web Protection, the Content Filtering, the Document Backup, etc., are virtually the exact same applications across all MSPs.

Remember there's only a few ITSM Platforms to choose from!

So, your network protection is just as good—***if not better***—from TRS than the services you would get from any other MSP.

The only real difference is the fact that TRS Actually Cares about the best interests of your organization!

Which is one of the main reasons why I built the TRS "***Only Pay For What You Get***" Hybrid Managed Services offerings.

I've built this specifically to help Small Businesses and Nonprofits, *just like yours*, get the Managed CyberSecurity, Computer Support and Network Protection they need at rates they can actually afford!

With three different tiers: Fully-Managed, Co-managed and DIY, we even help you control all of the additional costs by working with your team (as available) to be the hands onsite and remediate problems that would've required a visit.

It is my goal to help every Small Business owner and Nonprofit keep as much of their money focused on their business, their missions, their outreach, and the greater good of their community!

I, personally, hate the idea that all your hard-earned money could be being spent towards paying the bills of (*or should I say, lining the pockets of*) an MSP that doesn't actually care about you!

As I've Just Proven… TRS Can Potentially Save Your Nonprofit Over 80% Per Month In Managed Services Fees, As Well As Easily Save Your Organization 1000's Upon 1000's Upon 1000's Of Dollars Every Year!

I would love to speak with you directly about how we can actually help your business or nonprofit protect and secure its network and systems…

Please reach out to me today:

Michael R. Baumann II
254-535-0490 (Cell)
michael@trsets.com