A TRS Technology Solutions Guide To Small Business Network Security!

Why Do So Many Businesses Get This WRONG?!!

BEWARE

We are living in a whole new world, full of all sorts of challenges and new threats to our well-being… and I am not talking about the pandemic.

I'm talking about the Cyber-Criminals, who every day, create new ways to steal our personal information and hijack our business data for a profit.

I'm opening this book – and hopefully your eyes – with some REAL stats that *should* scare the s#!t out of you.

It's unbelievable just how prolific all this has become, and just how close we all are to potentially losing everything: Professionally, Financially, and Personally!

THESE ARE (*UNFORTUNATELY*) VERY REAL NUMBERS…

AND THEY 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 should 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 sobering 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 any further, let me just make sure you understand what malware and ransomware are:

MALWARE = Malicious Software
Malware is the term that means any type of software with a malicious intent. There are many forms of malware, including Malvertising, SpamBots, Scrapers, Destroyers, & Ransomware.

RANSOMWARE = Data Hijacking for Ransom
Ransomware is a type of malware program that takes over your company's (or computer's) data and threatens to "Delete It All" if you do not pay the ransom.

On the previous page, you learned that one-third of all U.S. computers already have malware on them. You also learned that every day, 250,000 computers are affected by malware. The FBI says malware usually sits dormant for 250 days before it attacks. And, BY FAR, the scariest stat of them all: EVERY MINUTE, at least four companies fall victim to a ransomware attack… did I say, "every minute?" Because I meant, E V E R Y M I N U T E O F E V E R Y D A Y !!

Let's think about Malware this way:
If I were to tell you that someone from outside your company, someone you do not know, has installed some software on your computer, and now potentially has access to all of your files, all of your data, all of your keystrokes, all of your logins, including all of your connections to your personal and commercial bank accounts. How would you feel?

Sick, I'm betting.

What if I also told you that with many forms of malware they can also hear your conversations through your PC-Mic, and/or even see you through your computer's WebCam?

How ya feelin' now?

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.

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

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. Small Businesses seldom invest in adequate Cyber-Security.

In just a couple of minutes, I'm going to show you one of the biggest problems most companies are making with regards to Cyber-Security. And, it's not just a technical problem, it's actually a misunderstanding.

As you'll see, this same mistake carries over into the physical world. Fix this one thing, and I believe at least 80% of your problem goes away.

WE ARE LOSING THE WAR ON CYBER-CRIME.

We're losing simply because most people are not paying attention. Most don't even know how bad it really is. They certainly don't understand the enemy, or their motivations. ***Apathy is our real issue.***

Because "war" is fought at a government level, and the fact that there are no *literal* body bags, caskets or memorial services, we are not giving this "War on Cyber-Crime" an appropriate level of concern.

Maybe even because so many of us are directly related to (or friends with) the brave men and women at Fort Hood who have been deployed, and fought in real battles – some we know and love even making the ultimate sacrifice… Maybe, that's why this "invisible" enemy doesn't seem real.

Cyber-criminals are not shooting at us, or at our friends and family… At least not exactly. But there are literally millions of attacks made every day. "Cyber-shots" fired as an attempt to hack in and steal our data.

Every company relies on data to make money. Everything is digital. Everything we do is digital. We've built our lives on digital information. BANKING - ENTERTAINMENT - EVEN HEALTHCARE - ARE ALL DIGITAL.

AND IT'S ALL CONNECTED... WHICH MEANS IT'S ALL ACCESSIBLE.

It doesn't matter if it has a password. It doesn't matter if it's encrypted. It doesn't matter if it's behind a firewall. These types of security options are no longer enough for today's sophisticated cyber-attacks.

As we continually move forward in a digital world, we expose ourselves, and our data, more and more. Moving forward - *digitally* - is necessary, but this also means moving away from traditional perimeter security.

As we allow for easier remote connectivity and mobility, including a Bring Your Own Device (BYOD) and Internet of Things (IoT) – open computing – architecture. We exponentially increase our exposure. And the problem is, you can't control your data in someone else's cloud.

You can't lock-down the network your employee is using at their home, or at the Starbucks. You don't have any control over the network you're using at the airport, or the hotel.

Your systems and networks, by design, will face the open Internet. Your company no longer has any definable perimeter. Security Must Change.

The value of data is changing rapidly and must be understood. Any data that you possess, on – or is accessible by – your computer, is at risk.

Chances Are ONE-IN-THREE That You Are Already Exposed!

The good news is, a lot of what the enemy is doing and using to steal your data and disrupt your business can be stopped, or at least slowed. Once you have a better understanding of who the enemy is, what they are doing, and how they're doing it, you will be in a much better position to protect your data and not become a victim.

With a few basic security principles and a change in mindset, you can start to build a culture of security, both at home and in your business. One that will send criminals to the business next door where leadership failed to take the steps provided in this book.

Like with a home invasion, if your home looks well protected, the criminals will continue down the street to a seemingly easier target.

In just a few pages, I'll show you what's happening and how to start protecting yourself from major losses, both at your business and in your personal life, as well. It won't cost you a fortune and won't require you to become a super-technical cyber-security geek, either.

By applying a few simple principles and starting to think about security in a new way, your life will be greatly simplified. You will be able to continue your journey in this Digital World with much more confidence.

UNDERSTANDING THE WAR ON CYBER-CRIME

This is a war no one sees. The War on drugs is evident. People of all ages –YOU CAN SEE – are using and selling meth, crack, heroin, etc. While drug dealers are not always easy to catch, law enforcement knows who they are. It's just a matter of time before they get caught.

The problem is, arrests are slow and proliferation is fast. We'll probably never win this war, but we know where it is and how to avoid it.

The war on terrorism is harder. We're often far behind their planning, but our government intelligence agencies are pretty good at picking up communications and thwarting terrorist attacks.

But, as we saw on 9/11, and other more recent bombings and mass shootings, it's hard to tell one person from the next, until it's too late.

Technology often aides these terrorist groups in secret communications and covert planning, but this is not a cyber-crime issue. In most cases, terrorism is a federal security issue or maybe even a military operation.

Data Security: War on Cyber-Crime is a Different Kind of Issue

It is a war we are losing. Mostly because of a pervasive unawareness about what is happening, and why it's happening.

Because there are no *literal* body bags, few are paying attention to the threat. Instead, we continue to build our world on digital platforms, with a seemingly blatant disregard for protection. Often sacrificing even minimal security for enhanced speed and perceived performance.

Soon, our entire world will all be online, easily taken and mis-used for someone else's profit. You could – ***without any exaggeration*** – lose everything: professionally, financially, and personally.

We've all heard stories of the "dumpster-diver" who found a piece of paper with just enough information on it to steal an identity. Stripping their victim from just about everything they own.

Identity theft is a common occurrence with Cyber-Crime. And, in this new Digital World, it's only getting easier for the criminals and worse for their victims. Victims can easily lose a bunch of money, maybe even their business, or their good name. Depending on just how bad it gets, the collateral damage often includes losing friends and family.

My hope, as you read this book, is you gain a better understanding of the war we're in. So you can take action – the steps necessary – to secure both your personal and professional life.

THE PRICE OF INACTION IS UNKNOWN

Maybe it's Identity Theft. Maybe your data gets hijacked and requires a huge ransom. Maybe all of your clients are sent fake invoices. Maybe you've already been compromised and don't even know it.
Regardless, more connectivity in this digital world means greater risk. The various weapons, strategies and tactics of this war have proved (time and time again, every single day) to be powerfully destructive.

This is a war we can't stop with brute force. It's going to take some rethinking, and the development of new habits.

AND IT ALL STARTS WITH YOU. YOU MUST ADJUST HOW YOU WORK AND HOW YOU THINK ABOUT YOUR DATA SECURITY.

YOU MUST UNDERSTAND THE VALUE OF YOUR DATA

Some of your data is worth money. Some of your data is actual money. Some of your data, as it is right now is very valuable: credit cards, bank accounts and investment information, etc. Some of your data is only valuable when it is added to other information already compromised: like dates of birth, mother's maiden names, favorite pets, etc.

The reality is, it doesn't matter how *you* define the value of your data. What matters is, because of the new growing use of Data Aggregation, YOU MUST KNOW ALL DATA IS MORE VALUABLE THAN EVER BEFORE.

Early hacking efforts were focused on bank accounts and credit cards. But, they are no longer the only datasets worth money. As businesses collect more and more data, Hackers are finding more and more ways to make money with it.

We already know, way too many of us are putting way too much of our personal "business" out on social media. Where we are, what we're doing, who we're doing it with, etc. ***#LOVING LIFE*** and ***#BLESSED***

Today's sophisticated Hackers can learn a lot just by sifting through all of this social media data. Which could then easily lead to pretexting.

> *Pretexting is when someone you don't know is pretending to be someone who knows you, with the pure intent to deceive you.*

Can you say ***#HATING LIFE*** or ***#HACKED***
Your Personal Data can be used to buy things you'll never see, put you into debt in ways you won't believe, and can even allow someone else to become you, just long enough to take out a loan in your name.

Your Intellectual Data could be worth a fortune overseas. You come up with a great new invention, and someone steals your plans, creates it and sell it overseas (for cheap), and there's nothing you can do about it.

Your Financial Data has always been a target. But even worse, today's Hackers are coming up with all kinds of ways to get people (even your employees) to send them money. Ransomware is just one example. There is also email wire fraud using simple tools, like fake invoices:

> *Maybe you remember the story from February 2020, where Shark Tank's Barbara Corcoran lost almost $400,000.*
>
> *Social Engineering Scammers tricked Barbara's bookkeeper into paying a $388,000 invoice because it looked like it came from Barbara's personal assistant.*

US companies have lost $26 Billion through email wire fraud since 2016.

Your Accounting Data, employee payroll and customer payment information are all at risk. Every day, credit cards are being taken, wire transfers are being made and banking credentials are being stolen.

Finally, your Customer Data, is worth money. Your customer lists and their payment information is like gold on the Dark Web.

Your customers expect you to protect their data, ESPECIALLY when it's sensitive information that could cost them a bunch of money, or cost them their job, their status, or disrupt their personal life.

SIMPLY STATED:
ALL DATA IS AT RISK! HACKERS CAN PROFIT OFF OF ALL OF IT.

When they profit, you lose – BIGTIME. When a Small Business reports a hack, there is a 60% chance they will be out of business within a year.

Unfortunately, the same technology that Facebook, Google and Amazon use to so effectively market to you, Deep Machine Learning and Big Data Analytics, also introduces a whole new level of risk, by helping exponentialize the value of even the smallest tidbits of data.

Deep Machine Learning refers to computers that use AI (Artificial Intelligence) to profile/predict things far beyond what people are doing.

Big Data Analytics (also known as Data Aggregation) is the compiling of large amounts of data, which can then be analyzed and used to figure out all kinds of things about a person.

In the hands of the wrong people, these systems can do major damage. From manipulation to pretexting, a person or company, can be quickly stripped of their money, integrity, reputation, and even their business.

YOU MUST RETHINK SECURITY

I can try and scare you with high impact horror stories all day long. Some will be moved, some won't. It's common for people to use fear as a motivator: where they focus on the shocking impact that others have endured, while they're trying to convince you to do something.

However, the real issue, ***you have to overcome to best protect your data and business***, is your own *perceived* likelihood of an attack.

If you do not have an accurate understanding of your likelihood, it's hard for you to imagine that these types of horrible cyber-crimes would actually happen to you and/or your business.

The Truth Is: Surreptitious Attacks Prey on the Uninformed!

Just because you look around and don't see any issues, or anything suspicious, and none of your employees are voicing concerns, does not mean you're OK.

It's kind of like a heart attack… Once you feel it, it's too late!

And again, just like a heart attack, there are certainly preventative measures you can take to help minimize the overall risk.

Ideally, you would keep all of your software up-to-date; guard yourself from malware; and have a solid backup strategy.

You can hope you won't need it, but you better prepare like you will.

As we move forward, into the main section of this book, I'll be showing you the One Big Mistake, which is foundational to just about every breach. Fixing just this one thing is your best overall chance of surviving all of the growing cyber-threats.

But before we dive into that section, let me just say that society, as a whole, misunderstands Risk and Security.

My goal, in hand-delivering this book to you, is two-fold:

(1) to help you become more informed about just how SERIOUSLY BAD cyber-crime has really become, and…

(2) to help you move from zero and/or minimal protection to adequate and/or *hopefully* better than just "good enough."

LET ME BE PERFECTLY CLEAR HERE: THE OLD WAY OF THINKING THAT FIREWALLS, PASSWORDS AND ENCRYPTION IS ENOUGH, IS WRONG!

As eluded to before, every day technology improves our lives. But at the same time, every day, criminals figure out ways to exploit this technology… finding vulnerabilities in the code.

Now, before I go any further, I cannot *NOT* say this… And what I'm about to share with you is *not* the One Big Mistake, but it is so commonplace, and so rampant throughout the small business community, I must take a few moments to shine some light on this, because SOMETHING HAS TO CHANGE!

Did You Know:
"The Majority of Cyber-Attacks <u>DO NOT USE</u> Sophisticated Hacking Techniques."

More often than not – especially with regards to the hacks perpetrated against small businesses, ***just like yours*** – if the hacked computer would have just been UP-TO-DATE on their software and security patches, or even had proper, and current, anti-virus programs and spam controls in place, they would not have been compromised.

Do you understand what that means? Just a simple, basic level of protection with a proactive mindset could thwart – ***if not even eliminate*** – the likelihood of you and your company becoming a victim.

LOOK, IF YOU ARE:

- contracting with Fort Hood, or the government, ***in any way***…
- dealing with sizeable financial transactions on a daily/weekly basis, like a car dealership, a mortgage company, or even an investment/financial planner… or…
- engaging as a contractor for (or a service provider to) any major U.S. corporations and/or major U.S. government contractors (like General Dynamics, Lockheed Martin, or Raytheon)…

YOU ABSOLUTELY HAVE A TARGET ON YOUR BACK!

However, most of you reading this are an owner of (or a leader in) a small, Central Texas community services business, or nonprofit. The likelihood that some major cyber-mafia (on the other side of the planet) is directly targeting your business is low… very low.

Meaning, we can agree that for the most part, your organization is not being singled-out and directly targeted, like those listed above.

But what is happening: 1000's of small businesses – JUST LIKE YOURS – are falling victim to crude, unsophisticated cyber-attacks EVERY DAY.

Petty cyber-criminals, and their rudimentary ploys, are winning big with most small businesses, simply because the small business leaders are naively unaware, and/or not investing in, and/or not updating, even the simplest levels of basic cyber-protection.

Whether it's a lack of awareness, or simple neglect, the truth is, if you're not ACTIVELY ensuring and confirming daily (or at the very least, weekly) that all of your software (from your operating systems, to your applications, to your anti-virus tools) are up-to-date, then the likelihood of you, and your organization, being hit by even the most elementary of today's cyber-attacks, is high… VERY HIGH!

THE ONE BIG MISTAKE

There are many contributors to every type of attack, both digital and even physical attacks, but this One Big Mistake is foundational to so many disasters. I truly believe if you fix just this one thing, at least 80% of your problems go away.

As you look back at history, *literally* through centuries of war and criminal activity, you might presume that we, as a society, understand security… at least physical security.

But this old way of thinking is making this Big Mistake even bigger. Homes and computers are broken into every day. Their security safeguards are no match when this one principle is being violated.

You may be surprised when you see what actually protects your house, and even more surprised to see what actually protects your data.

Things Are Getting Worse

These past few years have been violent. Mass shootings, murders and random acts of mayhem, in general, are becoming more and more frequent. Some are terrorist driven. Most are just crazy, angry people.

We can't stop these attacks, at least not easily. In most cases, these people are not open to reason or negotiation. They have a cause, it's violent, it's sick, and unless stopped, they'll carry it out, regardless of the cost. You cannot negotiate with people like this.

But again, this one principle of security – when applied correctly – greatly reduces the likelihood of disaster. When left out, criminals, terrorists, and crazy people have their way, and we all pay the price.

What is this one key element of securing both physical and digital assets that most people seem to be missing from their security strategy?

Well, let me ask you this: Have you ever taken the time to think about what actually makes something secure?

THE HOME ANALOGY

I like to use the Home Analogy because it's easy. Most of live in houses. Most of us feel safe in our homes. *I hope you do.* And most of us can easily relate to the aspects of securing and protecting a home.

My home isn't bulletproof, but it's pretty safe. But let's just evaluate how safe our homes really are.

What secures your home? If I were to start listing all the components of your home security strategy, we might come up with a list that looks like this:

Locks	Alarm System	Dog
Doors	Motion Detection	Gun
Windows	Monitoring Service	Police
Fence	Camera System	Insurance

You might have some or all of these things, but hopefully you've invested in the one's that matter most, based on where you live.

Security has to take into account your location, your assets, and even your relationships.

I'm sure we can agree, that in general, the list above is what people rely on to protect their homes. But, when you look deeper into how security works, you'll quickly see these *things* are not what primarily secure your house. You've been told they do, you've spent money on them, you've placed your trust in them, but you've been somewhat lead astray.

Locks, Alarms, and Dogs don't secure your home. So what does?

There is actually a system at work behind these security controls. It's a system that flows Left-to-Right, comprised of:

PROTECTION - DETECTION - RESPONSE

All three are required for a security program to work. It must be well-timed, and it must flow in sequence (left-to-right). If it doesn't, your security plan will surely fail when put to the test.

PROTECTION, DETECTION and RESPONSE

Perhaps you've never thought about this actual sequence, but this is how security works. All three are necessary, but one must be nearly perfect. It must have the right components, and they must be tested.

PROTECTION	DETECTION	RESPONSE
Locks	Alarm System	Dog
Doors	Motion Detection	Gun
Windows	Monitoring Service	Police
Fence	Camera System	Insurance

All three columns are needed, but there is a definitive order of importance and timing to make it all work.

I can tell you, when asked which column is the most important, most people will choose the wrong column. But it's not really their fault. It's what they've been told (*forever*). Most people choose Protection.

If you chose correctly, you chose Detection. Response is a close second, but Protection is actually third. Which is almost always the exact opposite of how most people vote.

I don't think anyone would argue that their home can't be broken into. Most criminals are looking for opportunities to go undetected. The less they are seen and heard, the more damage they can do, or assets they can get. It doesn't take too much effort to determine which houses are empty during the day; and which of those houses have alarm systems.

The second most important column is the Response column. But not just any response will suffice. ***It must be a Real-Time response.***

By Real-Time, I mean it must be fast enough to counteract the crime.

At your house, that may be 10-minutes. At a bank, that may be an hour. In computer time, it's nearly instantaneous. *An Immediate Detection and a Disabling Response must be present.*

Let's Look At Data Security

Most computers are protected by passwords, firewalls and encryption. Some of the better protected systems even have Email and/or Spam Filters. But notice how all of those fall into column one: Protection. *They all claim to keep people out.*

A physical security system requires all three columns, but depends mostly on column two, Detection. Data Security follows this same process. It just needs to be exponentially faster. In fact, Detection in the digital realm needs to be extremely fast, and much more robust.

Data is (digitally) invisible. There's no way you can ever expect to detect a cyber-crime, let alone stop one in progress, without special Detection and Response tools, designed specifically for that job.

Before I go on, I would like you to consider this:

Your home may be in a safe neighborhood. Your home may even be in an *extremely* safe neighborhood, like a gated community, with constant neighborhood patrols and private police.

But here's the point to consider:
Completely regardless of where you plug your computer in – your office, your super-safe home, even the Wi-Fi down at the local coffee shop – your computer is *NOT* in a safe neighborhood.

Once it's connected to the Internet, your computer is connected (and may even be available to) some of the absolute worst, corrupt, immoral, self-indulgent, evil criminals and crazy people from anywhere across the world.

THINK ABOUT THAT. WE ARE ALL CONNECTED.

Once you're online, you are now connected to all kinds of people: the richest and the poorest; radicals, conservatives and anarchists; even serial murderers, child molesters and sexual predators; people who love you; people who hate you; people who would kill your family in front of you just to watch you scream; AND THEY'RE ALL JUST A CLICK AWAY.

Scary isn't it?! Please, don't think about that kind of stuff for too long, you may never want to go online again, BUT… You should be thinking about better monitoring your children's online access. (***For Sure!***)

YOU CANNOT TRUST ANYONE YOU MEET ONLINE! Electronically, any person can pretend to be any other person they want. Truly evil could easily pose as a precious angel with the most giving soul.

ALWAYS BE WARY. ALWAYS BE SUSPICIOUS. ALWAYS BE VIGILENT!

Anyone can easily be the opposite of what they say they are. The pictures are not real. The videos can be faked. Which is how Social Engineering works: Collect Data; Make Connections; Build Trust; Draw The Victim In; Get What You Want; and…

ALL WHILE REMAINING TRULY ANONYMOUS!

Which brings us back to Computer and Data Security…
People are primarily driven by Power, Money and Sex. The Internet is the gateway to all three.

You've been told passwords will keep your data safe and encryption will keep your transmissions secure. You've been told that CHIP and PIN technology on you credit cards keep them protected and the FDIC will insure your money. You've been told firewalls will keep people off of your network and facial recognition as the password on your iPhone will keep people from accessing your personal life.

Everything you've been told about security is only partially true.
Passwords keep the petty cyber-criminals out. They don't stop Hackers. Firewalls will block the constant bombardment of Auto-Bot attacks.

They don't stop Hackers. Encryption makes your data harder to read, but it won't stop Hackers from accessing your most sensitive data.

HACKERS DO NOT CARE ABOUT YOU… IT'S ALL ABOUT THE DATA!

The only way to stop these criminals is to have a properly implemented SECURITY *SYSTEM*: Protecting, Detecting and Responding.

Let's go back to the Home Analogy. Look at your home for a minute and imagine the following scenario:

It's late at night, you and your spouse are abruptly awakened by your alarm. The siren is blaring loudly as you scramble to your feet. Your alarm is connected cellularly to the monitoring service – Signal Sent; Signal Received. Seconds later, the alarm company is calling to see if you're OK. At that moment, you hear footsteps charging down the hallway towards your bedroom… Now What Happens?

The alarm might scare the average criminal, but not all… What's your response plan? Remember, response must be Real-Time. Police are minutes away (5 at best, 15 at worst). If the cops were Plan A, what's Plan B? ***With no back up plan, security fails***. Sure the alarm went off; you got the phone call from the monitoring service; police are being notified and directed your way; but what will you do regarding the immediate threat charging down the hallway?

If you and your spouse are at work and the kids are at school, and then the alarm goes off, how will you know you've been hit? Unless the monitoring service calls the police – and somehow by the grace of God, they get to your house in time to stop a burglary – or a neighbor runs over to your house prepared to stop the intruders, assets will be stolen.

If the intruder runs into your neighbor unexpectedly, the situation is likely to escalate. What's your response plan now?

In the case of a mass shooting, detection is immediate, people know right when the first shot is fired. (*It is sad that I have this stat, but…*) the average active shooter incident is 11 minutes. SWAT cannot respond

that fast. Regular police may not be able to respond that fast. Unless there are armed people onsite – and ready to respond immediately – the security plan will fail.

Law enforcement cannot stop an incident in progress unless they are already there. Their job does not involve Preventative Detection. Which means you must be trained and ready in the event of an attack.

When it comes to data protection, the same is true. It happens so fast, human detection is almost meaningless. Plus, you as a small business owner can't just look around the office and see if any data is missing. Which also means you can't just assume that everything is OK. By the time you do detect an issue, it will be too late.

The average detection takes months, often more than a year. FBI says the average is 14 months. TJ MAXX took about three years. Target, Home Depot and JP Morgan all took about three or four months.

Real-Time Detection And Response Are Necessary If You're Going To Secure Anything! Good Security Happens when all nine boxes in the chart below converge into One Seamless Security Program.

It Won't Be Completely Technical, and…
IT CERTAINLY *WON'T* BE IMPENETRABLE.

But it will take you from your False-Sense of Security to a Detection Strategy, followed by Real-Time Response. This is the type of program that will allow you to stop most of the threats that will come your way.

	PROTECTION	DETECTION	RESPONSE
ADMIN			
TECHNICAL			
PHYSICAL			

PROTECTION. Like the home analogy, these controls help keep things out. Firewalls, passwords, encryption, etc. are all forms of proactive protection, designed to keep unauthorized users away from your data.

DETECTION. At this point, something has broken through your protective barriers. The faster you can detect the breach, the better.

RESPONSE. Once detected, time is short. A Real-Time Response will automatically block suspicious traffic. It will also alert your designated Security team/person who can then respond properly.

ADMINISTRATIVE. This refers to the security at the End-User level, including controls like: Sign-In Logs; Security Policies; and ongoing User Awareness Training.

TECHNICAL. Firewalls; Intrusion Prevention Systems; Intrusion Detection Appliances; Automated Response Tools; and other computerized, data security devices and applications.

PHYSICAL. Actual physical security protocols protecting the servers and network equipment, like locked doors with access control and monitoring options.

The Gartner Group estimates that over 75% of a company's security budget is spent on column one: Protection.

AND THERE IT IS… THE ONE BIG MISTAKE; THE ANSWER TO THE QUESTION POSED AS THE TITLE OF THIS BOOK…

"Way too many businesses invest too much into the Protection Layer, and almost completely neglect the most important aspects of a truly functional Security System/Program: Detection and Response."

Yes, you need layers of Protection. But, as you have probably already figured out by now, there's no real way – especially in any kind of cost-effective manner – to make the first layer (Protection) bulletproof.

And the truth is, "pretty good" protection works.

Your house probably has doors and windows designed for energy efficiency, not asset protection.

Your home has no real security without detection. Sure, you may have a fence, but someone can climb it. Sure, you may have a door, but someone can open it – even if it is locked. Sure, you have windows, but any $5 hammer from Walmart will get someone in.

The idea that locked doors and windows will deter a determined intruder is clearly wrong thinking. So again, the point is, Detection is the key – but followed very closely by Response (Real-Time Response).

First, you have to know that something has happened, then, you must be able to respond before it's too late.

Let me switch gears (slightly) and go back to a point I was making earlier

YOU MUST UNDERSTAND AND SECURE YOUR DIGITAL ASSETS.

The data your company relies on is mostly intangible and invisible. It's digital, not physical, and it is highly valuable.

Imagine your company is a car dealership, and over the weekend, someone broke in and stole the keys to one of your cars and drove it off the lot. (A) You would know it almost immediately. (B) There is easily a tangible value. (C) There is probably a standard procedure to follow to report a car as stolen: *First you call the police, file the stolen vehicle report, get the report, send it to the insurance provider, etc.*

BUT… in the Digital World, even if your dealership's most sensitive data is in a locked room, in a locked data rack, on a secure server with multiple levels of authentication and encryption, it can still be stolen.

You know why? Because the data is not really "*in the server*." It is IN, ON and AVAILABLE to any device that has access *to* the server.

Even worse than that, unlike the physical asset (your car) your data can be stolen while still remaining on the server. So, (A) how do you even know data has been stolen (or would you ever)? (B) Do you know what the value is? And (C) do you have a procedure to report the theft?

You simply cannot live in column one. Think about your house again. If someone jumps the fence and kicks the back door in, they've bypassed your Protection. But, if the alarm goes off, the Detection has done it's job. Response is next. If it takes 8 minutes for the police to respond, and it's just you, your spouse and your kids… what's the plan?

There are no easy answers. But – *back to business* – the protection of your data is your responsibility… and when Protection is not enough, ***YOU MUST HAVE DETECTION AND REAL-TIME RESPONSE.***

DETECTION IS ONLY AS GOOD AS THE TIMED RESPONSE PLAN.

Fixing the One Big Issue requires you to understand and acknowledge that the Hacker is always going to be one-step ahead. Like with physical break-ins, you can't really keep people out, so a move to Detection with Real-Time Response is necessary.

IF YOU THINK YOUR BUSINESS IS AN UNLIKELY TARGET… YOU'RE PROBABLY WRONG.

Not because I'm saying you, for sure, have a target on your back, but because of just how prolific all of this really is.

Hackers send out millions of old and new malware every day. Every day some 250,000 computers are affected by malware. Every day these attacks get more sophisticated, all in an effort to go undetected.

While there are certainly some unsophisticated and blatantly obvious attacks perpetrated by what we may believe to be the novice cyber-criminal; this does not mean that the obvious email is not an elaborate ploy, designed to get us looking one direction while the master at this digital "slight-of-hand" is actually doing something else.

Cyber-criminals may not all be evil geniuses, but some absolutely are. Well-practiced, well-prepared and definitely skilled at cyber-attacks… But even more important to know, is most cyber-crime is perpetrated by large groups; Cyber-Mafia and/or Cyber-Sweat-Shops, if you will.

If your business has done little to none with regards to Cyber-Security, and what you have done is just with the basic column one (Protection) aspects, ***there is a high likelihood you have malware on your systems***.

IN REALITY:
If you have not already deployed a Detection and Response focused Security System/Program, then your likelihood is 100%.

It's already happened. One in Three (30%) of U.S. computers are already infected. How many computers does your business have?

Is your data secure? In most cases, probably not. To believe otherwise is to risk everything you've worked for to this point. The Hackers' tools are powerful. Social Engineering always gets in. New technology and more automation opens new doors, and more vulnerabilities every day.

YOU CAN'T STOP HACKERS!

You can only get better at detecting data theft and stopping it before its too late.

You need to develop a Security Plan: a road map that will guide you from your current state to a future, more secure state.

Your goal must be to have a balanced security architecture. One that offers an appropriate level of Protection (based on the value of your digital assets), with specialized tools to provide early Detection, and a Real-Time Response plan that can counteract before it's too late.

To do that, you're going to need to know where your company data is. A Digital Asset Inventory, of sorts. Who has the data? Who uses the data? Where it sits or transmits… etc.

Next, you're going to have understand the value of your data. Different types of data are worth more or less, to you and the Hackers.

If your company needs direction regarding Digital Data Security, to help make appropriate decisions for Protection, Detection and Response-

enabled Data Security Systems, Programs and Applications, I would be more than happy to help.

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.

It's my goal to shift the viewpoint of Cyber-Security away from the idea that it's a product you can just buy, install and then now you're safe.

Cyber-Security is a system, with a definitive process. It requires an investment in Protection, Detection and Response. Designed specifically to Minimize Risk To An Acceptable Level. Then, Maintain Low Risk, with Immediate Alerts and 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 SECURITY OPTION OUT THERE My system is created in such a way that you only pay for the services you're actually getting. It's not – at all – based on a high, per device or per user fee that supposedly includes some level of additional service.

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

Please reach out to me today:

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

I would like to leave you with one last analogy…

THE ROCK CLIMBER

The rock climber wants to do something that in many ways seems impossible: taking on cliffs 1000's of feet high, and overhangs that defy gravity. He may spend nights sleeping while suspended from ropes anchored by small metal objects placed in cracks in the rock walls.

To achieve this, the climber invests in a helmet, special shoes, ropes, camming devices, anchors, carabiners, and a sling to carry his gear.

When the ascent begins, the climber (wearing his shoes, helmet and harness) begins to place metal anchors into the rocks, securing his ropes, as he works his way up. With the exception of the shoes, the gear is never actually used to support the climber – unless he falls.

All of the gear is designed for safety, not insurance. If the climber falls, the rope, already secured, will tighten, held by the anchors in the rock, and will support the climber, stopping the fall, long before disaster.

Rock climbers enjoy purchasing safety equipment. They look for new technologies that will provide greater security, allowing them to take on bigger challenges.

The climber invests in safety so he can mitigate his risks and decrease the likelihood of danger… This allows him to do what seems impossible.

If you and your business are going to continue the "climb" to new heights in today's Digital World, you too must invest in appropriate safety and security tools, designed to Protect, Detect and Respond… BEFORE IT'S TOO LATE!

I have the perfect solution to help you mitigate your risks and maintain a low likelihood of breach, designed (*and priced*) specifically for small businesses to help keep your business from taking a disastrous fall.

CONTACT MICHAEL TODAY!

If You're Not Ready To Speak With Michael Just Yet, Then Please Download The Second Book In This Series At: https://core6plus.com/cs-pdr-2

Delivered By Your Friends At:

TRS Technology Solutions

CORE 6+ BUSINESS NETWORK SECURITY PLUS

We don't see problems... **We See Solutions!**

Michael R. Baumann II, Director of Operations
TRSETS.com | 501C3TI.org
Physical: 1202 Rio Blvd | Bldg 6 | Killeen, TX 76543
Mailing: Post Office Box 725 | Killeen, TX 76540
TRS: 254-526-8900 | 501C3TI: 254-780-0310
Email: michael@trsets.com

501(c)3 TECHNOLOGY INITIATIVE