SBT SMALL BIZ THOUGHTS
by Karl W. Palachuk

Security Sales 2021:

Stop Selling New Stuff the Old Way

A Workbook Dedicated to Your Success

Karl W. Palachuk

Security Sales 2021: Stop Selling New Stuff the Old Way
By Karl W. Palachuk

Published by

Great Little Book Publishing Co., Inc.
Sacramento, CA
www.GreatLittleBook.com

Security Sales 2021:
Stop Selling New Stuff the Old Way

Karl W. Palachuk
October 2020

Everything about the threat landscape has changed during the past five years – except, perhaps, the way you design and sell your security services. I hope you will use this guide to refresh your entire approach to creating and selling security services.

With luck, you will redesign the way you sell the security services that are needed in the modern environment.

This workbook is not intended to be a resource that you breeze through in an hour to transform your business overnight. It is a place for you to take notes that will lead to internal conversations. Many of these topics are very complicated and will take a great deal of thought and discussion.

My goal here is to help you ask the right questions to begin the difficult process of reformulating your cybersecurity sales process.

Contents

Introduction . . .

This checklist is intended to help your team work through a major revision of your cyber security offering – literally from the top down. The "top" means your company's goals around your cyber security offering, and your vision for how you will get there.

We also examine how sales department and service department goals are aligned with company vision. You really do need to go through these exercises if you want to avoid a free-for-all with different departments working against each other – even if unintentionally.

Next, we focus on building or rebuilding your offerings. It may be that you already have the perfect offerings and you wouldn't make any changes. Great. At a minimum, you will verify that that's still true.

In Section Three, we talk about building the back end. That means all the software, processes, procedures, and documentation internal to your company. This is necessary so that you can deliver "the bundle."

Next, we look at the Sales department. In the never-ending cycle of selling what you intend to deliver and delivering what's been sold, a well-documented sales department is key to creating a successful customer experience.

Sections Five and Six focus on your future and current clients. You will define your ideal client going forward, and then use that ideal to measure the clients you already have. This will be a huge step in becoming the new brand you want to become, with higher standards of security and compliance.

Finally, you'll need to create a big checklist to execute all of your decisions. And that big, big job brings all the decisions to life.

Vision and Mission

→ Do not skip this section!

(Having said that, the actual process of defining your company's vision for the future, and the mission that create that new reality, are outside the scope of this document. You may have to go off for a lengthy series of meetings to clarify these things.)

Definitions

Purpose: Why does you company exist? Why are you doing what you're doing?
(Note: "Money" cannot be the answer. What's the real purpose?)

Vision: What would the world (or at least your world) look like if your company is successful at fulfilling its purpose?

Mission: What is the action plan to make your vision come true?

Three Layers of "Mission"

In very practical terms, it takes three layers of "mission" for you company to implement a long-term success strategy. First, there must be an over-arching corporate or company-wide purpose, vision, and mission. Then, in very practical terms, your sales and service departments each have to create short, medium, and long-term goals that promote the corporate mission.

For the next year, you should have specific, measurable goals that move your company, and your sales and service departments, closer to your overall vision of success.

Write these down:

For the year 2021

In support of these goals, you should also have short-term goals for each quarter.

Company Goals for the Year:

1. _____

   Q 1 goals: _____

   Q 2 goals: _____

   Q 3 goals: _____

   Q 4 goals: _____

2. _____

   Q 1 goals: _____

   Q 2 goals: _____

   Q 3 goals: _____

   Q 4 goals: _____

3. _____

   Q 1 goals: _____

   Q 2 goals: _____

   Q 3 goals: _____

   Q 4 goals: _____

For the year 2021

You should have a parallel set of goals for the Sales Department to support the company-wide goals (annual and quarterly).

Sales Department Goals for the Year:

1. _____

   Q 1 goals: _____

   Q 2 goals: _____

   Q 3 goals: _____

   Q 4 goals: _____

2. _____

   Q 1 goals: _____

   Q 2 goals: _____

   Q 3 goals: _____

   Q 4 goals: _____

3. _____

   Q 1 goals: _____

   Q 2 goals: _____

   Q 3 goals: _____

   Q 4 goals: _____

For the year 2021

You should have a parallel set of goals for the Service Department to support the company-wide goals (annual and quarterly).

Service Department Goals for the Year:

1. _____

   Q 1 goals: _____

   Q 2 goals: _____

   Q 3 goals: _____

   Q 4 goals: _____

2. _____

   Q 1 goals: _____

   Q 2 goals: _____

   Q 3 goals: _____

   Q 4 goals: _____

3. _____

   Q 1 goals: _____

   Q 2 goals: _____

   Q 3 goals: _____

   Q 4 goals: _____

Note: It is VERY important that you write these down, talk about them, and make them real. How will you communicate and verify alignment going forward?

Build (Rebuild) Your Offerings

You need an overall strategy about cybersecurity and sales. Again, this may require quite a bit of time, but the result will be a solid, consistent approach to cybersecurity that will achieve several goals. It will be:

1. Consistent
2. Easy to describe to clients
3. Easy to describe to technicians
4. Easy to document
5. Easy to measure compliance
   (with internal standards as well as NIST or other external standards)

Here are some building block questions to help you define your offering. Let's start with the highest and lowest possible configurations.

Step One: What does perfection look like? If you could create the perfect cybersecurity offering, what would it look like? How many components would it have? How would you document a secure site? How would you document compliance? How would you guarantee ongoing compliance?

Let's assume perfection is not possible, due to various constraints (time, money, personnel, the vagaries of the world).

Make notes here. Summarize your thoughts here. Use this to prepare a written policy.

Step Two: What does failure look like? In this case, we can simply define "failure" as unacceptable. In other words, when is security so low that you simply cannot be involved? For example, a client refuses to pay for a firewall. Or a doctor refuses to pay attention to HIPPA (in the U.S.).

Rather than saying, "I will recognize the line between acceptable and unacceptable when I see it," you should define a handful of scenarios that represent your definition of unacceptable.

NOTE: This is a great example of aligning goals between the company, the sales department, and the service department. Do not let your sales people flirt with the line. They need to understand that this line does not fit with your overall goals. Supporting factors include liability, insurance costs, company profit, etc.

Make notes here. Summarize your thoughts here. What is *unacceptable*? Use this to prepare a written policy.

Step Three: The technical offerings. Once you have defined the upper and lower limits, define the technical specifications for your tiers. You might only have one tier, but experience has shown that two or three tiers are best for sales as well as customer satisfaction over the long run. For our examples, we'll use the classic Silver, Gold, and Platinum.

For each level, define what's included. Traditionally, from a security perspective, this tiered approach has amounted to three *tiers of security*. In my opinion, this is because we have traditionally thought about the problem from a "products" and technical perspective.

Please note:

I HIGHLY Recommend

that you do not offer three tiers of security!

Imagine yourself standing in front of a judge and explaining that you know what a secure service looks like, but you sold the client less than what they needed. Now imagine yourself explaining that to your insurance company after they just paid the client's insurance company for the data breach.

Don't worry about explaining it to the client. They're busy hiring someone else to take care of their security.

Okay. So, if you want to offer three tiers, but you don't want to offer three tiers of *security*, what do you do? Think about it. It's really easy.

What business are you in? You're in the IT service business. If a prospect can buy security from anyone, what can they only buy from YOU?

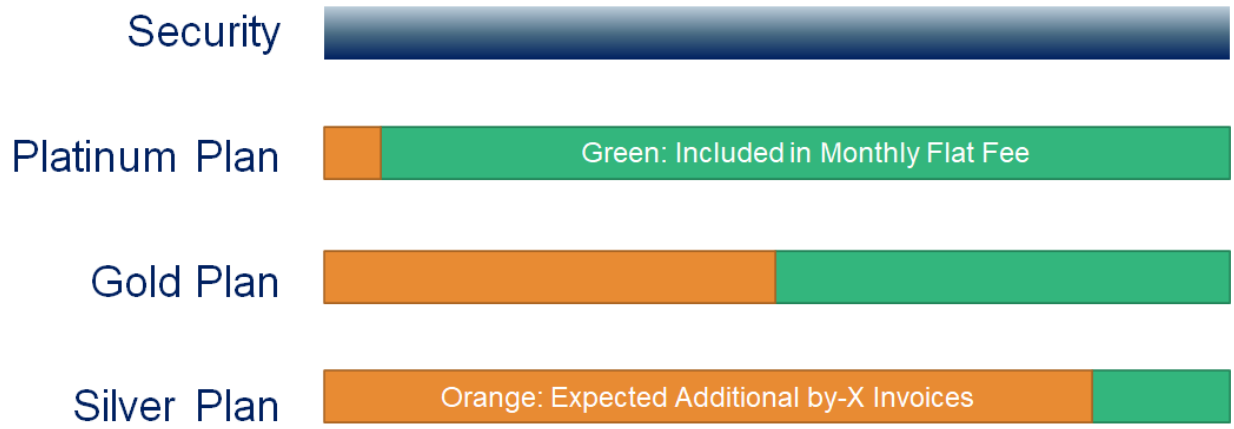
I encourage you to define three **levels of service**.

Let's assume that you will always provide that best cybersecurity that you can. Basically, you're going to get as close as you can to the "perfection" discussed above. Great.

Now, the client doesn't have to worry about whether their company is secure. Neither does their insurance company, nor your insurance company.

Once you start thinking in terms of service levels, building these levels is very easy. It's just a different way of looking at the world. And it's already being done by many managed service providers. This "new" way of looking at security isn't about *whether* you'll provide all the security a client needs, it's about how much is included in a flat-fee plan and how much is billed hourly (or per incident, or by the widget).

Here's what I mean. Let's start with *all the security a client needs*. Now, build your three tiers around how much *service* is included, or not. Everyone gets great security. Some pay more in flat fees and less in hourly.



Make notes here. Define three levels of service (not security). Start with notes here, but break out the Excel and create a well-thought-out document that you can use for internal training, sales, and service.

Example:

Service	Silver	Gold	Platinum
Monitoring	✓	✓	✓
Patch management	✓	✓	✓
Backup	✓	✓	✓
Patching Backups	✓	✓	✓
Dark Web Scans	✓	✓	✓
O365 “Premium”	✓	✓	✓
Anti-Virus	✓	✓	✓
Spam Filtering	✓	✓	✓
Cloud Storage	✓	✓	✓
Ransomware Response		✓	✓
Managed Firewall		✓	✓
Compliance Documentation		✓	✓
Remote Labor		✓	✓
Onsite Labor			✓
Disaster Recovery			✓
Quarterly Training Onsite			
Technology Roadmap Meetings	$999	$499	Included
etc.			

Template:

Service	Silver	Gold	Platinum
	✓	✓	✓
	✓	✓	✓
		✓	✓
		✓	✓
			✓
			✓
			✓

Step Four: Technical training and maintenance. Part of building your new offering is determined by the ongoing costs of maintaining your offering. This includes training your technicians, and potentially training sales people as well. Ongoing maintenance includes managing databases, servers, agents, updates, and so forth. On some platforms, this maintenance is minimal; on others it is quite time-consuming.

Make notes here. Define additional Sales Training that will be required with the solution you are adopting.

Make notes here. Define additional Technical Training that will be required with the solution you are adopting.

Define additional maintenance that will be required with the solution you are adopting.

Step Five: Legal, compliance, and insurance. In the 2020's, one of the biggest changes you'll see is that we cannot build an "offering" from a purely technical perspective. In addition to the discussion of how-to are the discussion of legality, compliance, documentation, and how all of that affects our insurance policy.

Again, you see why this has to start at the top and must include both the sales and the service departments. Long gone are the days when you could install a server, collect a big check, and leave the system for someone else to maintain. All of this has to be taken into consideration today.

Note, also, that documentation regarding compliance and insurance automatically adds a cost because it adds labor to the maintenance side of the equation. Remember that you're no longer offering levels of service, so the paperwork and compliance needs to be documented and done no matter what. Is it included in Platinum, done during business hours under Gold, and invoiced in Silver? How will you do this piece?

Make notes here. What are the requirements you will need to meet to provide these services and comply with all applicable laws? (Some of these may only apply to a specific niche, such as accountants or healthcare.)

What are the requirements you will need to meet to provide these services and comply with industry-standard compliance requirements? (Again, some of these may only apply to specific niche clients.)

How will you document your cybersecurity installations to verify the legal and compliance requirements, and meet the insurance-related requirements to keep your insurance policy active and enforceable?

Step Six: Customer Service. The final step in defining your offering is to look at all of this from the customers' perspective. Your clients will never understand most of what you do or why you do it. So, beginning with the sales process and proceeding through to setup and monthly service, they need to have a *consistent experience* with your company around cybersecurity.

I love to remind people that branding is **everything you do**. Every single customer experience reflects on your brand. So, the way you sell and deliver cybersecurity needs to be defined, documented, and executed with *intention*. If sales people and service technicians "do their own thing," they are building their brand, not your brand.

Make notes here. What is you public messaging around cybersecurity and how you implement it? What are the key points? In particular, which key *words and phrases* should be relied upon by sales people, technicians, front office personnel, and customer service reps?

Build the Back End

Finally! The techies have been waiting to get to work. Now it's time.

You need to settle on the overall framework for delivering the total solution defined above. Which solution(s) and software will you be investing in? Which vendor(s)? Will you buy into one unified solution, or a variety of separate tools?

Remember, the closer you get to full integration, the lower your overhead. But that also means you might be giving up one of your "favorite" tools because you don't want to bolt it onto an otherwise-integrated package.

Whatever you decide, do so with intention. Your conclusions should be profitable, of course, but also consistent with the company-wide goals as well as sales and service department goals.

You also need to build great processes and procedures. How-to checklists will guarantee consistency in designing, implementing, and maintaining all systems your company builds. Consistency is one of the hallmarks of security! SOPs – standard operating procedures – are a key element of a truly secure system.

From SOPs, it's a short step to great *documentation*, which is the key to compliance. You can have a system that "is" secure from a technical perspective. But it's not *known* to be secure until it's been documented. Most compliance standards also include ongoing maintenance as part of their standard for ongoing compliance.

Note: You may have to adopt some new SOPs if your company is transitioning from levels of security to levels of service. In the past, you needed to document which pieces of your solution were included at each price level. Now, you need to track whether a specific service (labor activity) is included at each service level. It's not more difficult. It's just different.

Building processes, procedures, and checklists can be a bit time-consuming. I recommend that you develop these as you go along. Always look back to the vision, mission, and goals defined above. And keep having those ongoing discussions to verify that everyone understands how your SOPs drive consistency with the bigger vision.

At some point, you will adopt one or more security standards. These might be as commonplace as PCI* and GDPR,* or as specific as HIPPA.* Many companies around the world are choosing the NIST* Cybersecurity Framework to guide their service

delivery plans, documentation, and ongoing maintenance. The basic reason for this is: It's a widely recognized, widely applicable, government-defined standard that can be used in defense of your actions (in court, in arbitration, with insurance audits, etc.).

No matter which standard(s) you adopt, service department personnel must either acquire outside training on the framework, or develop and document internal training on the framework. Again, this is a cost that should be taken into consideration when determining the total cost of implementing your solution.

The sales department needs to understand all of this *enough* to develop client-facing sales materials and presentations. If you don't have non-technical descriptions, someone has to come up with them.

[If you are tempted to start a castle and a moat analogy, I recommend you turn over this task to someone thirty years younger than yourself. Just sayin.]

* Alphabet Soup:

- PCI – Payment Card Industry
- GDPR – General Data Protection Regulation
- HIPPA – Health Insurance Privacy and Portability Act
- NIST – National Institute of Standards and Technology

Make notes here. What solutions and software will you be using to build your cybersecurity solution? Which vendors are involved? How many "connectors" will you need, and who provides them?

What additional training will be needed on the standards you adopt and the solutions you adopt? Make notes about which training will be **purchased** and which will be done **in-house**. Early on, these will be best-guess answers. Plan to revisit this discussion.

Outline your process for creating, storing, and updating processes and procedures related to the new solution(s). Have a plan! Documentation is central to ongoing compliance.

Define Your Ideal Client

Who will you sell to? Who will you *not* sell to? Do you need a specific minimum per client per month?

You will need to define exactly who you want to sell to. For example: Many companies end up trying to sell a high-end solution to clients who can't afford it. These clients might be perfectly willing to buy something, but cannot afford the thing you put in front of them.

Other prospects don't believe that compliance "applies" to them. So, they will never agree to a solution that provides all the protections YOU need to do business.

How will you define the clients you really want to go after? And how will you verify that you're consistently selling to the right people?

Create criteria. Write it down. Make it real and measurable. Create a checklist to verify that you are talking to the right prospects.

Make notes here. What does your "ideal" client look like? If you already have ideal clients, that's great: What do *they* look like? Start with this list, but add as many measures as you can think of. Once you have the big list, you can pare it down to the most important factors.

Ideal Client Features (draft)

Size (Revenue) _____

Size (# Employees) _____

Size (# Endpoints) _____

Size (# Servers) _____

Minimum monthly Revenue _____

Willingness to meet Compliance _____

Cloudy Friendly _____

Ideal Client Features (continued)

Use specific software _____

Willing to pay in advance _____

Interesting projects _____

They are a growing company _____

Have a budget (or willing) _____

Other _____

Other _____

Other _____

Other _____

Other _____

Notes:

Review Existing Clients

Using the criteria created for identifying your "ideal" client, evaluate your existing clients. Among other things, examine (and document):

- Budget constraints
- Attitude toward security/compliance
- Willingness to do things your way
- How easy are they to work with?
- Do they pay invoices in a timely manner?
- Are they frustrating to deal with?
- Are their projects technically challenging?
- Are they irritating?
- Are they profitable?

If your existing clients are not up to spec with your newly-defined offerings, that's not bad: It's a great way for your sales staff to learn how to position your new offerings in front of an already-friendly audience.

If you are committed to the overall process, then your existing clients will need to either come up to spec or transition to another IT service provider.

Step One: Evaluate Existing Clients. Grade them on their "fit" as an ideal client. (Note that this includes the list from the "ideal" discussion as well as the criteria just listed.)

I encourage you to have every employee from all departments evaluate every client they have interactions with (including service, sales, front office, administrative assistants, and even the bookkeeper).

Size (Revenue) _____

Size (# Employees) _____

Size (# Endpoints) _____

Size (# Servers) _____

Minimum monthly Revenue _____

Step One: Evaluate Existing Clients. (continued)

Willingness to meet Compliance _____

Cloudy Friendly _____

Use specific software _____

Willing to pay in advance _____

Pay invoices on time _____

Interesting projects _____

They are a growing company _____

Have a budget (or willing) _____

Willingness to do things your way _____

Easy/Frustrating to work with _____

Profitable _____

Best Guess:
How likely are they to sign up for the new offering? _____

Other _____

Other _____

Other _____

Other _____

Other _____

Other _____

Other _____

Other _____

Step Two: Take Action with Existing Clients. Once the "grading" is complete, you'll have clients who fit into several categories, including:

- Not a good fit with the new offering
- Most likely Silver
- Most likely Gold
- Most likely Platinum
- Could fit with some [major/minor] technical changes
- Could fit with some behavioral changes – money
- Could fit with some behavioral changes – non-money
- etc.

Next, you need to literally build an action plan around all existing clients. The ultimate goal is to get everyone who can be a good fit into the new offering as soon as possible.

Important safety tip: I *highly discourage* you from letting some clients stay on the old offering or on the old pricing. You need to move to consistency with the new offering as quickly as you can.

One of the worst things you can do is to destroy your own profit margins by having a different price and different service offering for every client. Sales people don't know what to do with that, customer service doesn't know what to do with that, and service technicians don't know what to do with that. Ultimately, the "Every client is unique like a snowflake" approach is not scalable. It literally limits the size and profitability of your company.

Your task, therefore, is to develop a plan to convert every client you can to the new pricing. I recommend the same strategy here as I do in *Managed Services in a Month*: Start with those who you think will not sign, and those who you think will sign for the Silver offering.

You want to start with the folks you think will opt-out or opt-low for two important reasons. First, you will be surprised at how successful you will be. Changing IT service providers is a pain in the neck. If your clients like you (and they do), then they want to stay with you. The only ones you will really lose are those who were looking for an out before you started any of this.

Second, and more importantly, there is less at stake with these folks, and it will give you a great opportunity to polish your sales process. All of those low-end folks will have questions. At first, you will have fumbling, stumbling answers. As you get the same questions again and again, your answers will be smoother and more consistent with the big picture.

Write down all those questions! If you can, write down your answers. You might even use a recorder to transcribe your answers. Go over this again and again. You will be better every time.

All of that "work" will make your first conversation with a most-likely-Gold client go very smoothly. Most-likely-Gold clients may have additional questions. Again, practice, practice, practice. Then repeat for most-likely-Platinum.

Basically, you're training yourself starting with the folks who are least likely to sign, but also those who you expect to bring in the smallest amount of recurring revenue. As your skills improve, you move up to the higher-value clients. ALL of this is good for building an effective sales process for prospects and strangers.

Finally, you need to move up to clients who you know – and you know they need to make some changes. Maybe they need to be easier to work with. Maybe they need to stop arguing about money and give you a credit card. Maybe they have to understand that that 2012 Server just isn't going to be covered on the new plan.

No matter whether a client is an easy sell, hard sell, possible-Silver, possible-Platinum, or whatever else, you need a plan for each client.

I'm not going to repeat all the advice from the chapters in *Managed Services in a Month*, but you're basically going to follow that entire "Client Sit-down" process. If you don't have the book, go get it. It's $30 and will save you hours of trial and error.

Action Plan. For each existing client, build a strategy for discussing your new options and getting them to sign a new agreement. Try to sell everyone on Platinum, even those who you think are most-likely-Silver. You'll be amazed at how many sign.

Notes:

Build (Rebuild) the Sales Process

This follows on the previous section, but is a lot more involved.

In order to verify that the solution you deliver fulfills all requirements regarding legal issues, compliance, insurance, technical issues, and company goals, your sales department will have to understand each of these and develop a solution-based sales approach.

Will you have a core offering for each of the three tiers, and then customize? Or perhaps two tiers will be pre-packaged offerings and the third will be customized by definition.

If your sales department is used to selling based on tiers of security, there will be a serious shift to tiers of service.

Every piece of the sales process has to fulfill all company goals, including addressing the right audience while prospecting. Your brand will be maintained when you have consistency from first contact to completion of implementation. That literally starts with sales.

Remember that line between acceptable and unacceptable cybersecurity? It is a danger sign when a sales person consistently wants to discuss that line. It means they are talking to the wrong clients, and pushing the bottom of your company standards. It may be best to encourage them to help another IT service provider redefine *their* level of unacceptable.

Make notes here. How will your sales process change in order to introduce existing clients and new prospects to your new cybersecurity offering? Will specific sales training be required? Plan to revisit this discussion quarterly until you feel like you've got it figured out.

Create Your Big Tick List

Okay. Now you've got a rough plan for revising your offering, and your clients. And you know what you need to do regarding training for both the service department and sales department.

It's time to execute! And that means, you need to create the big **Revise Our Cybersecurity Offering Checklist**. You will need to note which tasks are to be performed by administration, sales, and service.

Actually executing the checklist will require a great deal of communication. And that's a lot more than one meeting. You'll need to communicate regularly to make sure you're all on the same page on all the details.

Start by simply going through all the notes and checklists from above.

Divide the work. The more you discuss this process with the entire staff, the smoother it will go. The front office staff needs to know why tech support is doing *this* and sales is doing *that*. Everyone needs to understand what everyone else is doing.

Revamping your entire offering and sales process is a big, big job. Don't screw it up by skipping the "Mission and Vision" section. Also, don't screw it up by thinking this can all be done by one person – especially the owner. You team needs to make this happen.

Plan to hold meetings as often as you need to. No one likes meetings, unless they are short and make your life easier. So plan on lots of short meetings. A handful will be longer, but most can be very short. Set measurable goals with dates and have people report back on a regular basis.

On several occasions, I have undertaken this kind of massive change. Believe it or not, I've found that one month is a good time frame. Two great examples are: 1) When our company was right around $1 million in revenue, we move all of our clients to flat-fee managed services in thirty days. 2) A few years later, we moved all of our clients to 100% cloud services in thirty days.

Note: In both cases, there was 100% buy-in from the top down. There was no discussion of whether we were making these moves: only how.

Ten Things You Need to Know about Selling Cybersecurity Today

1. Selling cybersecurity has to be part of a holistic approach.

- Bolt-on solutions and afterthoughts don't work in the 2020's.

2. Establish goals for the company, the sales department, and the service department.

- All department goals must support the company vision and mission.

3. Security has to include discussions of compliance, legality, and insurance.

- We no longer live in a world of purely technical solutions.

4. You cannot offer incomplete or insecure solutions.

- Because you cannot live in a world of purely technical solutions.

5. Rebuild your sales process around *tiers of service* rather than *tiers of security*.

- There must be an enforceable minimal level of security.

6. Pick a standard you can use to define your process and implement it consistently.

- You can't just make up this stuff anymore!

7. Your new approach, philosophy, and sales process will change the conversation around security.

- "Make do" and "get by" are no longer options.

8. Choose (or build) a back end with as few vendors and independent components as you can.

- Every "connection" is a maintenance point. (Remember, no bolt-ons.)

9. Define your ideal client.

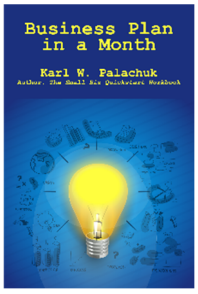
- Go get them! And if your existing clients are not ideal, make a plan.

10. Schedule a meeting for Fall 2021: Review all of this.

- Make this a never-ending conversation.

Resources

Please Consider These Resources from Small Biz Thoughts



Business Plan in a Month

By Karl W. Palachuk

Available exclusively on Amazon Kindle.

Your business needs a plan. You can't succeed without a plan. Very few people stumble around like Forrest Gump and make it to the top. In fact, zero people achieve that.

Managed Services in a Month

By Karl W. Palachuk

Available on Amazon, Audible, or smallbizthoughts.com.

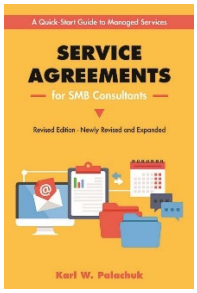
The ultimate do-it-now guide to getting started in managed services. Includes chapters on cloud services, bundling, and more.

Cloud Services in a Month

By Karl W. Palachuk

Available on Amazon, Audible, or smallbizthoughts.com.

A step-by-step, no-nonsense guide to building an extremely profitable cloud service business for the SMB market.



Service Agreements for SMB Consultants

By Karl W. Palachuk

Available on Amazon or smallbizthoughts.com.

Everyone knows it - spoken agreements aren't worth the paper they're written on.