Transformation of an Industry into a Profession

Thoughts on Revamping our Industry

Karl W. Palachuk

2021
Originally posted in May and June, 2021 on the Small Biz Thoughts Blog
Minor proof-reading updates June 28, 2021
https://blog.smallbizthoughts.com

Contents

Part 1: The Nine Pillars

Preamble

The IT Consulting industry has come a long way in the last twenty years. We are more professional, as a group, than we've ever been. We certainly have better tools, better organization, and better channel-focused vendors. I am honored that I have played some small role in the evolution or our industry.

But we also face greater challenges than ever before. I don't want to blame all of our problems on ransomware, but the explosion of ransomware in the last few years has forced us to shine a light on some long-standing problems within our industry. It has also sped up the inevitable march of legislation and regulation. And all of that has led to skyrocketing insurance payouts and premiums.

Unfortunately, the natural response to all of this is to address each element in isolation. But that is not the answer. We need to begin thinking about the maturity of our industry in a more holistic manner. Our response to ransomware, for example, is clearly tied to our diligence in managing client systems. And to insurance rates. And to regulation.

I've been thinking about the big, big picture. So, in this series of posts, I present nine topic areas that I believe are all inter-connected, and related to the overall professionalism and maturity of our industry. Please comment, share, and join in a discussion of these elements at a higher level. I present these thoughts as a starting place. But I really want our industry to tackle these questions and begin working together on creating a united front to address our problems.

Some of these will seem obvious, but others may seem unrelated at first. But, remember, I'm looking at all of this from a holistic perspective. What does it take for our industry to take a big step up in professionalism and participate in a future where we can thrive while providing truly valuable services to our clients?

Warning: A lot of people will be angry at what I have to say. Please post comments, share this and comment, or email me directly. I want to start a conversation about raising the bar for SMB IT professionalism.

One requirement is very clear, but rarely discussed: We need to take responsibility for the bad things happening in SMB IT, and in our industry. I'm not saying we started it, or that we are perpetuating it. But the default position of pretty much everyone in the channel is to treat our problems as if they are happening to us - as if we play no role. Well, that's simply not true.

We've all met people whose life seems to consistent of a Series of Unfortunate Events (to paraphrase Lemony Snicket). You've met them. One tragedy after another. In each case, they are the victim. No one could have foreseen this or that. Bad luck is everywhere.

The older you get, the faster you recognize this pattern and learn to run away from these people. Every bad thing in their life was someone else's fault, and all the bad things happened TO them.

Let's look at our industry. We don't create ransomware. It happens to our clients. We just fix it. We're not responsible for higher insurance rates. That happens because clients click on stuff, ignore training, and get ransomware. We're not responsible for government regulation and legislation. That happens to us because no one can do anything about viruses, malware, phishing, and ransomware.

In other words, the default is: We're not responsible for anything. Sh*t happens and we have to deal with it.

Except . . .

Lots of people in our industry cut corners. We try to save clients money and end up selling incomplete services. Lots of people sell "managed" services and deliver break/fix. Lots and lots and lots of small businesses have no real protection. Some consciously refused to pay for good tech support. But many of them have IT service providers who don't force them to do things the right way, or simply don't deliver the kind of preventive maintenance that will protect them.

From one perspective, we are totally caught in the middle with no way out. But I encourage you to consider another perspective: Figure out what role we can/do play. And then figure out what we can do about it. Legislation doesn't have to happen TO you. You can choose to get involved and shape what the future looks like. High insurance rates don't have to happen TO you. You can engage and find out the specific things we need to do to lower those rates.

Let me be crystal clear: YOU might do everything right, have great processes and procedures, and have a perfect record of avoiding ransomware for your clients. But you are still affected by the fact that our industry as a whole is doing a very poor job on this front.

If you want to sit back, collect auto-payments, and do nothing, that's fine. But you will then be choosing to let participants in the conversation decide the future of the industry, and your business.

Let's dig in.

The First Pillar: Profit

Profit is not the only measure of success, but it is a necessary one.

Depending on who you talk to, about 20-25% of IT Service providers are not profitable. At a minimum, they're breaking even, which is to say, "scraping by." I recently talked to a friend who is a member of the Institute of Management Consultants. When I told him this statistic, I thought he would be surprised. Instead, he said he doubts the numbers are that low. He says that most industries have more like 25-30% who fall into the category of unprofitable.

I know it sounds very hard to believe, if you're struggling, but there's no reason for this. If you have an unprofitable business model, that's fixable. If you have trouble with sales, that's fixable. If you lack skills, that's fixable. Basically, unless you are simply unwilling to make changes, your problems are fixable.

To be honest, when I talk to people who are struggling in this business, they are working very hard to figure things out. Very likely, they are working ridiculous hours and not charging clients for their time. So that loops back to the business model - which is fixable.

I believe it's important to talk about profit first because unprofitable companies tend to make bad decisions. When people feel they have to take certain clients, or have to take every client, they spend their time focusing on money to the exclusion of service, security, and what's best for everyone involved.

Unprofitable companies have lots of problems not directly related to money. They cut corners. They give in to clients who want to make bad decisions. They leave themselves open to problems, and therefore leave their clients open to bigger problems. They don't invest in their employees or see them as valuable resources.

If you're having problems with profit, you obviously cannot snap your fingers and become profitable. After all, no one is unprofitable on purpose. It takes a lot of discipline and focus to turn things around. You have to make hard decisions - like cutting staff and reducing expenses.

I address profit as the first pillar because it is truly the first building block to creating a solid base on which to build a successful, professional industry. Only a profitable industry can effectively tackle the rest of the elements addressed here.

As individuals, we must do what needs to be done to build successful businesses. As an industry, we need to work together to help define profitable standards and procedures. And one important piece of that is to avoid competing on price. Making yourself and others unprofitable just to gain market share provides no positive results to anyone.

The Second Pillar: Maintenance-Focused Support

Backup and Maintenance are the foundation of all IT service.

One very bad trend we've seen over the last five years or so is the failure to focus on preventive maintenance. When I wrote the first edition of Managed Services in a Month, my assumption was that all IT service providers had a "maintenance first" or "backup first" approach. That assumption turned out to be very wrong.

I stand by my original belief: Managed services *should be* focused on maintenance first. For me, that includes a fundamental focus on testing backups. In the big-big picture, testing backups is the single most important thing we do. If you test backups every month, you know two things: 1) The backup is working; and 2) Your team knows how to restore data when the day comes that a restore is necessary.

The second most important thing we do is apply all the patches, fixes, and updates. There's no secret here. No genius-level certification needed. Unpatched hardware has problems; unpatched software has issues; unpatched operating systems have troubles. Viruses and ransomware take advantage of unpatched holes, primarily in software.

So, no matter what else you do, you need to apply patches, fixes, and updates on a regular basis. If you track the news about the latest big ransomware attack, it almost always turns out to be a new attack on an old vulnerability. In other words: A properly patched and maintained system would not have been compromised.

I've posted before, but I'll repeat it here: Most people who call themselves "managed service providers" are not providing managed services. Many of them love the flat-fee subscription

model, but they are not providing the backup services or patching services that clients are paying for. Instead, they are providing reactive break/fix support and charging a flat fee.

This is very bad for all of us. You might be focused completely on preventive maintenance, but you are severely affected by the fact that many people in this industry are not taking preventive maintenance seriously.

Every single time there's a new story about ransomware taking down a city, a county, or a company of any size, I am stunned that this is still a problem. These stories only make the news because of one thing: Their IT support failed to provide effective patching AND their IT support failed to make sure they had a working backup. A BDR should be able to recover a system in 1-24 hours. Even an old, slow backup should be able to recover everything within a week.

But paying a ransom due to failures in IT support should never happen. Ever. We have solved this problem. Yes, I know there are new kinds of extortion-ware, but even those attacks can be virtually eliminated by proper patching.

Now think about this from a State- or Provincial-level government. What you'll find is that they see exactly what Kyle Ardoin, the Secretary of State of Louisiana saw: Government agencies (which are essentially small businesses) are paying for "managed services" and are still not protected from the most basic attacks. Patches are not being applied. No backup or BDR is in place. Or, the backup isn't working, but no one knows that because it's not being tested regularly.

Now consider this from the view of insurance companies. Businesses of all sizes are buying managed services, but they are still compromised. Ransomware continues to flourish. Patches have not been applied, so the attacks are successful. Backups are not working (or non-existent), so ransom has to be paid. Whether or not it's justified (we'll get to that), insurance companies want to hold the managed service providers liable for the damages.

Let me repeat myself: YOU might be doing everything right. But you are severely affected by the fact that so many IT service providers are not doing the most basic things necessary to protect their clients. You may have had a perfect, zero-incident year, but your insurance rates went up anyway. You need to care about the fact that our industry needs to take a step up.

Part 2: Education, Certification, and Core Values

In the last section, I introduced the need to revamp our industry and step up professionalism. I proposed the first two pillars: Profit and focusing on backup and maintenance first.

In this installment I address education, certification, and core values.

These are the natural elements of a profession. Think about any profession (teaching, accounting, legal, financial, etc.) and you'll find that the industry became professional when it adopted standards for continuous education, certification of experts, and adoption of some core values.

The background for all of these is the transition from amateur to professional. All industries attract new members from among interested amateurs. The road to professionalism starts with experience. But at some point, informal training and then formal education are needed to make the big steps in knowledge.

Certifications follow from education and provide acknowledgement that certain standards have been met. The more evolved the profession is, the more standardization there is on the focus of this certification. And while our industry is typified by change, we need to acknowledge that other industries also deal with constant change. I always joke with my tax accountant that every change in tax law should simply be titled, "The Tax Professionals Full Employment Act."

The specific elements of our areas of knowledge will change over time. Ultimately, the definition of an industry is determined by values and standards that guide the industry. The only real moral difference between people who make a living from ransomware and those who make a living selling office apps is the underlying core values about appropriate behavior in the market. And when an industry evolves into a profession, it has to have a public discussion about values.

Here, then, are the next two pillars.

The Third Pillar: Education

Education and certification are central to professionalism and continual renewal.

We all start out knowing nothing. And we all become masters of a few things. And, if we're lucky, we become excellent at several things and good at many things. No one can be a master of all knowledge. For almost any technology, there are many layers of knowledge. There's the one paragraph description, the 1,000 word discussion, the 350 page book, and the library filled with books.

One of the not-so-secret dirty little secrets in our profession is that people over-use Google to pretend they know more than they do. At some level, this is the very definition of an amateur trying to work their way into "semi-pro" status. Amateurs know just enough to figure stuff out. They are slower than professionals. Their solutions are less elegant. Sometimes they break more than they fix. But, ultimately, they figure it out and figure out how to do it better the next time.

All professions grow because hobbyists become amateurs, and amateurs (apprentices) grow to become professionals. Experience is one big piece of this transition. But education and certification are another. Anyone can stop growing at any point and simply stay where they are (amateur, apprentice, or professional). But for the true professional, "staying where you are" means sliding backward. The technology and business processes keep evolving. Without continual training, you cannot keep up.

At some point, there is a real limit to what an amateur can achieve. And you cannot be a master of all things. So, when you choose something to get good at, you need to dig in and educate yourself. That might include books, classes, or even formal schooling (a collection of classes).

Think about how we naturally learn technology. Take firewalls for example. You can dig in and "figure out" a lot about setting up a firewall. But you will never get beyond the "figuring out" level

without some real education on TCP/IP, ports, protocols, routing, and so forth. And there are multiple levels of education in each of these.

There is a fairly obvious period of being aware of your amateur status. At some point, you decide to either be amateur, semi-pro, or dig in and really become good with firewalls. Or at least one brand of firewall. But even if you decide to specialize in Fortinet or Sonicwall, formal education includes a great deal of generalizable knowledge. At some point, you learn a great deal about routing, filtering, and traffic management that goes beyond the brand of a specific product.

Some people tend to dismiss education and certification. Their argument sounds something like this: Anyone can spend a bunch of money, go to a "bootcamp," and get all their certifications in one weekend. Okay. There was a time when people did that.

But here's the reality: I've never met someone who passed seven or eight exams from Microsoft or Cisco who didn't also know a great deal about a variety of technology. Even if you cram for such exams, there is a moment in time when you knew the topic well enough to pass the exam. We all know that the real work of "knowing" something involves the daily application of what we've learned.

I've taken lots of Microsoft exams. Most of that information was never useful to me. But that arcane and archaic knowledge is still rattling around in my head. And I could apply that knowledge with just a little tune-up.

There are two kinds of education and certification in our industry - technical and business. Technical education is widely available. Vendors provide education on their own products and services. Some of it is free and some is for a price. Of course, Microsoft is the big example for most of us. If you are willing to dig around on their web sites and train yourself, you can get virtually all the knowledge they have to offer for free. Or, you can pay for officially-sanctioned training and get a good chunk of that data distilled into a day or a week.

There are also third-party training opportunities, but they are fewer. CompTIA probably has the most well-known training and exams. Third Tier and other independent organizations provide great training, but on a limited number of topics. Happily, almost all community colleges (and some high schools) provide a wide variety of technical training.

Business training is a little different. Vendors only train you on processes that promote their view of the world. You should be leery about adopting a business model based on the needs of your vendors. As brutal as it sounds, they only care about you to the extent that you use and sell their products and services.

Business-focused training is harder to come by. Many coaches and organizations provide training on the business side, but we have yet to see a really large organization offer business-focused training on a grand scale. Most of the coaches or communities you've heard of offer business-level training (myself included). But our industry could use some serious standards and increased consistency on this front.

As an industry that wishes to become a profession, we could advance a lot by agreeing on some standards for education and certification. At a minimum, we should focus a lot more on the training that's already available. If I had to propose a slogan for this campaign, it would be:

Google less. Read more.

In isolation, anyone can watch a YouTube video and see how to export a PST file. That's a far cry from understanding all the elements of migrating a client's entire operation to cloud services securely with zero downtime.

Read more. Google less.

The Fourth Pillar: Core Values / Statement of Ethics

Ethics and principles ultimately define an industry and build the path to the future.

Here and there throughout our industry, you might find a Code of Ethics or a statement of core values. But there are three common problems with such statements. 1) They tend to be very long, overly detailed, and therefore go unread. 2) They tend to be too vague and end up repeating a few meaningless phrases. 3) They tend to be hidden away.

At some level, we all have a vague sense that we share a set of values. I love to quote Bill and Ted's Excellent Adventure: "Be excellent to each other." And while we would all love to live in that world, it's just not real (yet). There are people in our industry who will undercut your quote, lie to prospects, and then bully them into paying a higher price even thought they promised a lower one.

I'm sorry to say that I have only appeared in court as an expert witness on three occasions, and ALL of them were to evaluate the appropriate behavior of other technology consultants. People in our industry do lie. They do steal intellectual property. They do take money from clients and not provide the services promised. Not you, of course. But you have to live with the fact that these people represent themselves just as you do - and clients have no measuring stick to compare the difference.

We need to adopt a handful of key values that we agree to be measured by, and which we can use to hold one another accountable. And while there's great value in something like Ray Dalio's Principles, a usable code of conduct needs to be brief in order to be effective.

Many dismiss the need for a common code of ethics, but our industry is surrounded by behavior that makes the need for such a code greater than ever. Money has an amazing power to increase the flexibility of some people's ethics. And, today more than ever, money is flowing through our industry in vast amounts.

When I first started consulting in the small business space, I felt like I had stumbled onto the wrong profession altogether. Again and again, I met prospects who had been ripped off by their previous IT consultant. Very often, hardware and software were registered in the consultant's name and not the clients. Eventually I discovered that this was done to take advantage of distributor spiffs, or because both hardware and software had been resold more than once, always sold as new.

The first time I ever met a Microsoft MVP, he casually mentioned that you can always "flip" an MSDN license and install something a client needs. There was a total disconnect between stealing in general and stealing software.

In another form of stealing, I witnessed time and time again that people took jobs they were not remotely qualified for, gave bad advice, and simply walked away when it all blew up. Many,

many times I took over networks after someone had over-sold the client, did a half-assed job of setting things up, provided zero documentation, and then simply disappeared.

Some will make the argument, "I'm honest. I act with integrity. Why do I care whether the whole industry has a code of ethics?" Well . . . because you work in that industry.

We make fun of the entire car sales industry, but we're basically in the same boat. If the perception is that "all" MSPs sell security management and then let ransomware attack their clients, that reflects on you. You might have had a perfect zero-bytes-compromised year. But when regulators and legislators are going after your industry, the actions of other players IS affecting your reputation.

One piece of the ethics puzzle is to simply have a code of ethics. But the more important piece is to agree to hold each other accountable (and to be held accountable).

Think about what a company values statement does within your company: It allows everyone to ask whether proposed decisions or actions are consistent with our stated values. A professional code of ethics is a public statement that says that we hold ourselves to these standards, and we invite the public to hold us to them as well.

I propose a few thoughts here as a place to start the discussion around a Professional Code of Ethics for IT Service Providers. Note that this is short enough to print on a single sheet of paper. I welcome your feedback and comments, especially if I left out some very obvious element.

A Draft Professional Code of Ethics for IT Service Providers

As a professional IT service provider, we pledge to:

- Be competent. IT Service Providers will work to stay educated and capable in all areas for which they represent themselves to be competent. They will not knowingly claim competence that they do not possess.

- Be honest. In presenting themselves to prospects, and in all engagements with clients, IT Service Providers will provide honest information about products, services, pricing, and related matters. This includes the accurate representation of work performed and the products and services offered for sale.

- Be forthright with clients. This includes registering client hardware, software, and services in the client's name and not the IT Service Provider's. It also includes providing the client with a reasonably useful copy of their network documentation. Implicit in this requirement is the fact that the client has paid for all of these things and that ownership or licensing should be in the client's name/possession. This also includes disclosing any possible conflict of interest between the IT Service Provider and the client.

- Be legal in all activities. IT Service Providers will follow applicable laws with regard to business operations, sales, data protection, privacy, and all other manners.

- Be professional. IT Service Providers will sign contracts with clients that are reasonable in nature and not intended to give an unreasonable or undue advantage to the IT Service Provider. IT Service Providers will conduct all business with the highest standard of ethics.

- Be fair. IT Service Providers will treat everyone (clients, employees, suppliers, vendors, etc.) impartially without regard to ethnicity, age, gender, disability, sexual orientation, nationality, language, religious beliefs, or political beliefs.

- Be discreet. IT Service Providers will sign non-disclosure agreements with all clients and employees, and work earnestly to protect client confidentiality and intellectual property.

Ideally, a profession-wide code of ethics should become something we all post on our web sites and publicly agree to guide us.

Part 3: Ransomware and How We Handle It

A great deal of this discussion about our industry, and where we want to take it, is triggered by the crises of ransomware, how we respond to ransomware, and how governments and insurance companies are responding to ransomware. And so far "we" don't have a response. Lots of vendors are selling lots of solutions. But none of them is really a solution: Each is a small fix for a small piece of a big, big problem.

As with so many things in technology, our response to problems consists of a big toolbox filled with various sizes of Band-Aids. But very little effort is put into taking a step back and looking at the big, big picture.

Here's a great example: Identity theft or credit theft. On more than one occasion I have posted photos of my driver’s license or credit cards online. People come screaming out of the woodwork because these things contain lots of information that can be used to "steal" my credit, open accounts in my name, etc.

But I don't care for a simple reason: I have made this information useless. Try to open an account in my name. You can't. Try to buy a house in my name. Try to take over my car registration. Try to use my credit cards. You can't.

You see, there are different ways to look at problems like this. "The data" genie is out of the bottle. I grew up in an era when my social security number was my student ID. I think it was published in the school directory. The birth dates and death dates of my parents are public information. My ex-wife worked for the State of California during roughly 1,000 incidents where all of our private information was stolen and sold on the dark web.

Your information is just as secure. So you are no more or less secure if you post your drivers license online. But you can take steps to make that information useless. You don't have to throw up your hands and say, "Oh well. If they want to break into my stuff, they will." And yet, that defeatist attitude is exactly what virtually everyone in IT says to one another - including MSPs, VARs, vendors, distributors, and even security companies.

I have written this many, many times over the last five years, but it's still true: There is absolutely no excuse for ransomware to take down a business or government agency today. The first time I created real-time data-mirroring between offices in Southern California and Northern

California, the setup was about $100,000 and monthly monitoring and maintenance was about $10,000. I was happy to do it.

That exact site could be backing up to a BDR with images in the cloud for a fraction of that cost today. (I hope they are.) What was once nearly impossible and extremely expensive has become simple and very reasonably priced.

The question is no longer whether we can secure all data but whether we are willing to. And that "we" clearly includes the client. Next time, we'll talk about insurance and government regulation. Clearly, if a client cannot afford to be protected, the IT Service Provider should not be held liable for the results of a ransomware attack. And, clearly, if a client can afford but refuses to pay for the appropriate systems, then the IT Service Provider should not be held liable for the results of a ransomware attack. But that's next time.

Now let's look at the next two pillars for our emerging industry: Defending client systems and our consistent response to attacks.

The Fifth Pillar: Defending client systems

Defending client systems and data is an ethical imperative.

I know a lot of people are not comfortable with the discussion of ethics and what's ethical. But I am. Maybe it's my "Arts and Sciences" education. But I think that professions do have some ethical requirements. For example, financial advisors should put their clients' financial interest first; they should not overcharge their clients; they should not steal from their clients.

All of that is actually based on a clear difference in knowledge. When you know more than your clients, you have the opportunity to recommend "solutions" that don't really increase security. And you have a great deal of power to remove yourself from taking the blame when things go wrong.

See the previous section on an industry code of ethics.

In the first installment, I made the case that basic maintenance and backup are central to our profession. Here I would take that up a notch. I believe we are obligated to defend our clients' data once they have engaged us. And a huge piece of this is based on that same differential of knowledge.

I've heard people make fun of clients who think that their data are automatically backed up because it's in the cloud, or with Microsoft. Similarly, they laugh about clients who think that mirrored drives or a RAID array are backups.

But here's the hard cold reality: If we want to be a profession instead of a collection of really smart people who all just happen to work in the same industry, we have to draw a line and take responsibility when the client cannot make correct decisions for themselves. If a client doesn't understand backup, and you do, you have an obligation to look after their interests. When a client doesn't understand security and you do, you have an obligation to look after their interests.

Your clients will never know what you know or understand what you do. They are professionals at dentistry, or law, or finance, or whatever. They trust you. They rely on you. They turn to you and ask, "What should I do?" You are morally obligated to give them good advice. Ultimately, what we do in this business is to help clients make good decisions about technology.

The funny thing about this discussion is that so many people immediately put it all back on the client: They refuse to secure their systems; they refuse to pay for it; they don't believe they're in danger. But that doesn't excuse you from your moral obligation.

This goes beyond you and the client. The "client's data" is often not the client's information to leave unsecured. The client's data probably includes their clients' information, medical records, financial information, intellectual property, etc. Your client has no right to wave their hand and decide that such information can be open to compromise.

We're seeing more and more compliance legislation all the time. It all boils down to this: Left to their own devices, many people will not secure their own systems or their clients' data. And further, compliance legislation acknowledges that society has a stake in securing that data - even if a specific company doesn't want to.

As an IT service provider, you don't have any choice. You are part of this mix. The players are you, your client, the government, and insurance companies.

So, protecting and defending this data is an imperative. What do you do when the client simply refuses to comply, for whatever reason?

Today, the best you can do is to have them sign a waiver of liability. But it is unclear whether such waivers are enforceable. As you probably know, almost every contract has limits on liability that are simply ignored. When lots of money is at stake, companies sue. Insurance companies sometimes pay out. And then they sue to recover their money. I'm not aware of any contract that has actually prevented a lawsuit.

And no matter what you do, you're still in the mix. Whether we like it or not, we need to work with governments and insurance companies on a formal process for removing ourselves from the mix.

It begins with acknowledging that creating data security systems and business continuity are imperative. Then, the client needs to be educated, to the extent that's possible. But remember: Some clients will never understand or accept the danger.

In the world of finance, there's a thing called a sophisticated investor. A sophisticated investor is someone who has lots of experience and knowledge in a variety financial dealings. So, for example, you might only be invited to consider a certain investment opportunity if you can document that you are a sophisticated investor.

We experience a similar thing in technology. If you're reading this, you're probably a sophisticated technology consultant. You know and understand certain things at a level that most of your clients will never reach. So how do you educate them sufficiently so they can make an educated decision to not protect their data?

Ultimately, you cannot force any client to buy into a business continuity solution or to protect themselves from ransomware, extortion-ware, etc. Today you have three options when a client refuses to protect themselves: 1) Take the risk that you'll get caught up with them, their

problems, and their insurance company. 2) Walk away and let someone else take the risk. 3) Stay and try to limit your liability.

There should be a formal process whereby you educate the client. And, if they choose not to protect their data, there should be a formal process - recognized in law - that removes you from liability.

This process cannot be haphazard. It needs to be a formal process. The insurance companies need to go along with it. And I expect they will, if it's done right. After all, the reason they're raising rates through the roof is that they're paying out massive ransoms because so many systems are simply not protected.

We will return to this topic below.

The Sixth Pillar: Response to our greatest challenges

A strong profession begins with consistent, effective responses to our greatest challenges.

In 2020, the world of compliance took a huge step in the right direction. And somehow, almost no one noticed. Every time I mention that the US Department of Health and Human Services has blessed the use of NIST CMMC for attaining and documenting HIPAA compliance, I get several requests for links.

[Okay. Just to get this out of the way, here are the links to start with:

- https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html
- https://www.hhs.gov/sites/default/files/cybersecurity-maturity-model.pdf
- https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf]

This is one example of the kind of thing we should be doing on several fronts. HIPAA (the Health Insurance Portability and Accountability Act) originally had no clear guidelines. It had no standards that could be built into a checklist. There was no way to document compliance. And, oddly enough, compliance could not be achieved without documentation.

As a result, "compliance" was simply determined by who sued or brought an action against a healthcare provider or IT professional. Finally, the DHHS move in 2020 made it possible to define compliance, create checklists, and demonstrate compliance. The documents above literally map CMMC actions to HIPAA requirements.

This is a great model that we can repeat in other areas. Again, with one eye on the government and the other on insurance companies, we can develop procedures that define appropriate responses. The basic formula is this:

Define the challenge. For example, stop viruses and phishing attacks from allowing data to be compromised, encrypted, and exfiltrated.

Define a set of actions and processes that define professional best efforts with regard to the task at hand.

Define procedures and checklists which, when implemented, will meet the requirements for best efforts.

Document the execution of these processes and procedures, and be willing to be judged by this documentation.

In a perfect world, we don't need the government to be involved in any of this. But, so far, our industry has spent more effort passing the buck and selling Band-Aids than solving the biggest challenges we have. We each come up with a set of different procedures, software, and services. And when it doesn't solve the problem, we confidently tell each other, and our clients, "There's no way to stop everything."

I go back to my original statement: There is absolutely no excuse for ransomware to still be a problem today. But instead of getting our arms around it and addressing the big picture problems, we spend our time playing whack-a-mole and making sure we're not the ones being sued for millions of dollars.

I see three obvious ways that action will be taken in the next few years. First, we can continue our uncoordinated attempts to apply patches here and there. This will result in the government taking action that solves some problems for the government but probably doesn't solve the actual problem. Remember: government agencies are getting hit at least as much as private businesses. They'll do "something" in response, even if it's not the best thing.

Second, the insurance industry will draft legislation and it will spread across the globe. This is actually the most likely response since the insurance industry is already well funded, well organized, and very experienced with lobbying. I assure you, their response will serve them very well. You will not find yourself relieved of any liability if the insurance industry writes the rules without input from IT service providers.

Third, we as a profession can begin to address the big problems with standardized processes and procedures that address the needs of our clients, government agencies, and the insurance companies. This approach might include getting some of these processes and procedures written into government regulations or legislation. It would involve engaging the insurance industry in discussions about what they need, and the role we play.

To be honest, a coalition of the IT service industry and the insurance industry may be the most powerful thing we can do. We could actually draw some lines around the obligations companies have to protect data, the liability that goes with that, the requirements for best efforts to protect that data, and the documentation required to verify where liability lies.

In many ways, we have accidently taken on liability for our clients' behavior by the response we have to security challenges. And now it's time to limit that liability and define the terms under which it can be lifted off of us and placed back on the client.

The only way to eliminate liability altogether is to eliminate risk altogether. Between ourselves, our clients, and the insurance companies, I believe we can define processes and procedures to reduce risks considerably, and therefore reduce liability as well.

I'm not saying it would be easy. But it could be done.

Part 4: Legislation and Insurance

For context, please see the previous posts. The first six pillars for an IT profession are: Profit; Maintenance-Focused Support; Education and Certification; Core Values and Ethics; Defending client systems; and Response to our greatest challenges.

Basically, we've been building a collection of actions that can help us all take a big step up from being an industry to a profession. The biggest problem we have is not ransomware per se: Our biggest problem is liability. We are stuck between evil programmers and insurance companies.

There are four major players in the SMB IT equation:

- You
- Your Client
- The Government
- Insurance Companies

By "you" I mean the SMB (small and medium business) IT consultant. You might call yourself an IT pro, a reseller, a VAR (value added reseller), a managed service provider, or other name. By "you" I do NOT mean large, enterprise-level consultant or IT-outsourcing companies.

Why the distinction? Well, there are three primary reasons. First, those very-large outsourced IT companies are really in a very different business. They are generally large, well-funded, with layers of management. And, to be blunt, they can take care of themselves.

Second, those large outsourced IT organizations do not have the same service model. As a rule, they sell IT-as-a-service to very large organizations, including companies with offices all over the country or all over the world. My first consulting gig involved working for one of these mega-corporations. Every year, the company buying tech support would put out bids worth many millions of dollars. And every year, IT outsourcing companies would bid to provide the most support for the lowest amount of money.

As a bit of a side note: Such companies tend to provide overall horrible support. They are the stuff of Dilbert cartoons and TV sitcoms about IT consultants. Their service model is almost opposite of SMB IT in all ways.

Third, those large outsourced IT organizations place very little (or no) value on the client relationship. Someone in the sales department cares about getting the client to renew a contract. Someone in management wants to meet performance targets so they get their bonuses. But pretty much everything else in the organization is designed to beat the metrics and close tickets without regard to making the actual end-user clients happy.

Yes, that's all my opinion. And one might say it's inaccurate. But I'd be happy to have that argument on stage in front of ten thousand users supported by those companies.

My point here is that SMB IT is different. We are not in the same profession as those folks. Even mediocre IT consultants at the small end of the market are almost obsessed with customer service. To be honest, we don't talk about this as much as we should - just for bragging rights -

because we are all hyper-focused on keeping clients happy. In fact, if you go back to Pillar number one, profit is often sacrificed in favor of customer service.

So, there's you. And then there's your client. Again, by definition, we are in the SMB market. As a rule, we don't support 30,000 desktops across fifty different offices. We tend to support between one and one thousand users in one to five offices. There are outliers, but the 1-500 seat clients probably make up ninety percent of all our clients. I'm sure Jay McBain or someone at Forrester knows the number. But you understand who your clients are.

Next there's the government. And, for most of us, that's a state- or provincial-level government. There are few federal or national level laws governing what we do. So far, most of the national level regulations have been around privacy data and financial data. But more laws and regulations are coming.

Most regulation and legislation is a step closer to home. State and provincial governments are actively looking around to see what they can do. Eventually, these things will work their way up to the national level, but for now we are seeing lots of proposed legislation at the state level. This is common with many areas of law, so we're gradually seeing a very normal evolution of regulation.

Basically, it's our turn.

Legislators read about companies and state agencies being attacked and brought down by ransomware and other cyber attacks. Of course, most legislators are from professions other than technology, so they have only a passing knowledge about what's actually going on. But it's their job to defend their constituents, their districts, and the tax payers' interests. So legislation is inevitable.

Finally, there are insurance companies. Believe it or not, insurance companies are more or less caught in the middle as we are. They wrote policies for problems they could foresee and measure (e.g., business interruption due to hard drive failure, or backup failure). They were not prepared for the massive growth in ransomware payouts in the last few years. Numbers are all over the place, but here's one: Bitdefender's Consumer Threat Landscape Report shows a 485% increase in ransomware in 2020.

https://www.bitdefender.com/files/News/CaseStudies/study/395/Bitdefender-2020-Consumer-Threat-Landscape-Report.pdf

Insurance companies are scrambling to respond. The requirements for a ransomware payout are becoming stricter. And insurance companies are pushing training for their clients. I have been pleasantly surprised at all the resources my insurance company makes available to me for cyber security training.

With this framework in mind, let's look at the seventh and eighth pillars for turning our industry into a profession.

The Seventh Pillar: Regulation and Protection

Recognition as a profession includes both statutory requirements and limits on liability.

I am a "minimalist" when it comes to regulation. I have a Master's Degree in Political Philosophy, so I could write a book on the appropriate role of governments in civilization. But sometimes you just have to face reality. And right now, for our industry, legislation is coming. The number changes every day, but I believe twenty-one states have proposed legislation that affects our industry.

We have a very simple choice to make on this front: Either jump in and try to influence the regulation as it comes, or do nothing and let that regulation happen to us. Given that choice, I strongly advocate jumping in and participating in the conversation.

Remember: Legislation goes both ways. That's why companies spend the effort to lobby governments. Given the Pillars I have addressed so far, we can identify some "gives" and some "gets" that might be included in government regulation.

[For this discussion, I will talk in terms of a US State legislative body. Similar processes would need to be followed in Canada, the UK, the EU, Australia, etc.]

First, and foremost, the SMB IT industry should be identified as a legitimate profession. That means there are some requirements. It also means there are some protections. The simplest way to be identified by name is require that a specifically identifiable group be registered with an appropriate state agency. Depending on the state, this might be the Secretary of State, Secretary of Commerce, Consumer Affairs, the Contractor's License Board, or some other entity. Each state is different.

Give: We register with the state. There would probably be a small fee for this.

Get: The state should maintain a database of registered IT Service Providers.

Second, the state may then regulate the industry. Specifically, I foresee that a state would require that all companies who do business with a registered IT Service Provider be required to sign a contract, enforceable by the state. This contract would then require that backup services be offered under every contract. And, of course, it would require that cyber security incidents be reported to a specific state agency or regulatory body. Again, this then becomes publicly accessible data.

Give: The state regulates us. This puts some limits on what we must offer.

Get: We have contracts with all clients, no matter how small, and there is an enforcement mechanism with the state government.

Third, the state should provide a way for a client to opt out of data recovery services, but also provide that doing so relieves the registered IT Service Provider from liability or responsibility related to a cyber security incident. Note: It should not be easy to opt out of backup and disaster recovery services. But if the client just plain refuses to buy such services, the IT Service Provider is not responsible for the consequences.

Give: We have to offer the services and educate the client enough that they understand what it means to opt out of such services.

Get: If there is a cyber security incident and the client has opted out of the appropriate protections, we cannot be sued by the client or their insurance company. (Note, also, that the insurance company can use this same legislation to deny or limit cyber security coverage to the client.)

We need to get ahead of this issue. We need to participate in our own well-being. There could be lots of details, of course, regarding the size of deals that must be bound by this legislation. But at least we'll all be playing the same game and everyone will know what the rules are.

The Eighth Pillar: Cooperation and Alliance with the Insurance Industry

A mature profession works with other professionals to safeguard ourselves and our clients.

Insurance rates are skyrocketing, primarily because the insurance companies don't have any choice. On the issues of addressing ransomware, cyber security, and insurance payouts, we find ourselves very much aligned with the insurance industry.

After all, insurance companies have seen ransomware payouts go from a few hundred dollars to several million in just a few years. Attacks are serious, sophisticated, and very highly focused. Insurance companies want to provide reasonable protection to us and to our clients. But when you go up against the essentially unlimited resources of the Russian government, it's hard to figure out how to win.

If we partner with the insurance industry, we can propose solutions that limit liability when client cannot or will not protect themselves. If we had a system like the one described above, it would allow us to be properly insured. Our clients would fall into three categories: 1) Not regulated, 2) Opted into backup and disaster recovery services, and 3) opted out of backup and disaster recovery services.

Those not regulated would also not be allowed to come after us or the insurance company. One obvious example of this: A client who only buys a phone system from you, the total cost is under a specified threshold, and they are not required to have a backup and disaster recovery system with you. So they might have one with someone else, but not your company.

Those who are regulated have a relationship now regulated by law. If they opt into backup and disaster recovery services, the insurance company and you both accept liability and insurance rates can be set. If they opt out of backup and disaster recovery services, then both you and the insurance company are protected from lawsuits that might arise from a cyber security incident.

I'm not a lawyer, a legislator, or an insurance agent. There are lots of details to be worked out. But I believe there's a big picture in which the IT Service Provider industry and the insurance industry have a lot of common ground and some powerful reasons to work together.

As with any professions, there may be times when we're on opposite sides of an issue and times when we're on the same side. In this case, I believe there is great value in being on the

same side and partnering up to protect more small businesses, create a reasonable balance of liability, and keep insurance rates at a reasonable and sustainable level.

Part Five: Building a Path to our Professional Future

We've covered the first eight pillars. That brings us to the future - which we'll need to create.

Whether or not you agree with the definition of Managed Services or professionalism that I've outlined here, one thing is true: There is a never-ending flow of people entering our industry. And, as far as we can tell, that will go on forever.

Again, when I talk about "this" industry, I mean SMB IT - not enterprise. Not big business.

For about the first fifty years of our industry, there were two common ways that people got into SMB IT. Either they worked for a larger organization and decided to get out while they could, or they started out as a tinkerer and fixer who figured out how to make a living with IT. It took a long time before SMB IT shops started having employees.

Most people who haven't been in the industry for more than fifteen or twenty years may not know that multi-tiered companies (with at least two layers of management) are a very recent phenomenon in small business IT. And since this aspect of our industry is so new, there is no established apprenticeship process.

In most industries, there is a somewhat standard path from newbie to seasoned professional. And we have a bit of this. But our industry has not defined paths for new entrants to gain experience and education that lead to specific job titles. The closest we've come is a series of technology-specific exams. Take a few exams on SQL Server and you can become a SQL administrator.

Ultimately, such technology-specific paths can never become professional paths. I have Microsoft certifications that go back to Windows 3.1 in 1995. A handful of that knowledge is still useful, but virtually all of it is time-bound and obsolete. Even the MCSE and Small Business Specialist certifications that were so valuable to my company ten and twenty years ago are just proof of knowledge once possessed.

If a modern IT business is maintenance-first and focused on a "managed service" model of service delivery, then we should be able to define requirements for both the specific technology of today and the more general business model for delivering that technology successfully and profitably.

The Ninth Pillar: Building a Path to the Future

A successful industry must build a path for newcomers to grow and thrive, constantly creating the next generation.

One of the ongoing problems I mentioned in the first part of this series is that IT professionals continue to sell based on the promises of managed service, but they continue to deliver break/fix. This happens, in large part, because they don't embrace the managed service business model. Perhaps they're unaware of what it entails; perhaps they just like the recurring revenue and don't really understand how to do all that maintenance-first profitably.

When industries are not professional, people just sort of "fall into" a certain job or business. Because they didn't take a path to the industry, each person comes from different experiences and education. They might be very, very skilled at what they do, but there's very little in common that could become the basis for a larger, professional approach to the industry as a whole.

Time and time again, when we find ourselves talking about books that changed our business and made us more successful, people say things like, "I wish I had found this when I first started my business." I heard that exact comment last week on a call. The book (not surprisingly) was *The Emyth Revisited* by Michael Gerber. I'm proud to say I've heard the same thing about *Managed Services in a Month*.

What we need is not a definitive library that everyone should read, but a general acceptance that there are some core concepts that define our profession. And here I begin to see the profession as something defined by some core business knowledge on top of the current technical knowledge.

Here's an analogy: Accounting. Lots of people figure out how to run QuickBooks, balance a checkbook, and keep track of income out expenses. They are amateur accountants. With enough practice in a specific area of accounting, they might become really good amateurs. But without proper training, they will not become professionals.

Accounting professionals take a certain course of training. They don't necessarily all read the same book. Each takes an Accounting 101 course that has SOME primary reading material and delivers the core concepts that introduce the student to the profession. Some of that knowledge is how-to, but it also includes a bit of ethics and a lot of practical advice.

Following this analogy, I am not advocating that a specific book or existing class be required for our discipline. I am advocating that some level of education on business philosophy for IT be included in training for our profession. We will always need technical training, but that will always become obsolete over time.

The non-technical training should define the current business models one might choose from. Break/fix and managed IT are both good, solid, profitable options. And anyone managing a professional IT consulting business should understand what each of these means, as well as the consequences of embracing one model over the other.

Finally, let's look beyond the technician. We all acknowledge that we've reached the point where we'd like to find an attorney who has worked with managed service providers before. They simply understand our business a little better. And we'd love to find an accountant who has worked with IT professionals before. And, in the 2020's, we're realizing that it's great to find an insurance agent who has worked with IT professionals.

When you look at it from that perspective, there are many element of our industry that are different from the rest of the service industry. We have specific challenges and skillsets. We have good, better, and best ways of operating our businesses and delivering services.

Now let's look internally. It would be great to hire an office manager who has worked with IT professionals - especially in managed services. It would be great to find a service manager who understand the managed service model. The same is true with sales people, administrative assistants, and (of course) technicians.

We are now at the point of our professional evolution that someone could enter a managed service business and find that there's an advantage to understanding our business model, and competing business models. One great way to acquire that knowledge is through formal training.

We need to embrace formal training in IT services and managed services as an important path to creating great job candidates and building successful businesses. And, through that process, we will continue to grow as a true profession.

-- -- --

This has been a lengthy series. Thank you to anyone who has read most or all of it. I would sincerely like to discuss next steps with anyone who wishes to move this profession forward. Agree or disagree: Let's have a conversation.

I am honored to be part of this industry. And as it makes its inevitable way to becoming a profession, I look forward to assisting in any way I can.

Please post comments and questions. And stay tuned for a few proposals to apply these nine pillars going forward.

:-)

A Summary of the Nine Pillars

For Transforming the SMB IT Industry into a Profession

The First Pillar: Profit

Profit is not the only measure of success, but it is a necessary one.

The Second Pillar: Maintenance-Focused Support

Backup and Maintenance are the foundation of all IT service.

The Third Pillar: Education and Certification

Education and certification are central to professionalism and continual renewal.

The Fourth Pillar: Core Values / Statement of Ethics

Ethics and principles ultimately define an industry and build the path to the future.

The Fifth Pillar: Defending client systems

Defending client systems and data is an ethical imperative.

The Sixth Pillar: Response to our greatest challenges

A strong profession begins with a consistent, effective response to our greatest challenges.

The Seventh Pillar: Regulation and Protection

Recognition as a profession includes both statutory requirements and limits on liability.

The Eighth Pillar: Cooperation and Alliance with the Insurance Industry

A mature profession works with other professionals to safeguard ourselves and our clients.

The Ninth Pillar: Building a Path to the Future

A successful industry must build a path for newcomers to grow and thrive, constantly creating the next generation.