MODERN CPA

Transcript for Podcast Episode: 011

Technology and Cyber Security Solutions for Small Businesses with Marc Umstead

Hosted by: Michelle Ward and Shawn Cahill

Guest: Marc Umstead

Michelle: We are Modern CPA. Our purpose is to provide valuable information to small business owners on our podcast Profit Points. We discuss business how tos, give tax tips and dig into real life experiences in the crazy world of running your own business. If you find this podcast helpful, then like subscribe and follow us on social media.

Michelle: Welcome everybody to our podcast Profit Point where we talk to professionals, industry leaders and small business owners about their journey and what they see in the world of being in business. And today we have Marc Umstead from Plus One Technology. And Marc, tell us a little bit about yourself.

Marc: Sure. So I'm the president of Plus One Technology. My firm works with small businesses to basically use technology to make their workflow and their business processes better and improve the overall, you know, security and reliability and productivity of their environment.

Michelle: Awesome. Awesome. So what size businesses do you work with? Do you work with one person businesses all the way to larger companies? Like what area?

Marc: So we yeah, we work with anybody from, you know, that has a, you know, one or a handful of employees up to, you know, what they call a co-managed environment where we're working with internal staff for companies that have, you know, 500, 1000, or 2000 people.

Michelle: Wow.

Marc: You know, maybe we're providing just some, you know, some services. But, yeah, we really run the gamut. I would say we focus on firms that are, you know, between ten and 50 employees, just kind of where, you know, most people, you know, a lot of firms fall. But, you know, we work with anybody.

Michelle: That's so great. So what brought you to start Plus One Technology and like what is your background? What found you going into business for yourself?

Marc: Sure. So it's kind of weird. You know, I grew up, being 40, kind of grew up when computers grew up. So I started when I was young working for an insurance firm, logging loans on pieces of paper, you know, writing down, you know, the information, you know, when it was filed. And, you know, people would then, you know, ask for, you know, well, we need the information on Bob Smith from, you know, four years ago. Can you go to look through a box of a thousand pieces of paper and find his information? And then I was just like, there's got to be a better way to do this. So that kind of started, you know, we're really but I'm not, you know, the most technical person out there. I don't I don't know everything when it comes to technology, but I am more of a workflow business process person. So it's about taking technology and actually making your workflow better, not worse. So I would you know, I kind of developed, you know, initially an Excel document to store all this information, easily find it, and then that kind of grew into a database. And then, you know, we kind of put everything in the company in this database to run it. So, you know, growing up, how do we make business processes better? Workflow better? How do you make people work faster? You know, more efficiently? Is really where, you know, I kind of grew up in technology, not, you know, coding software and all that kind of stuff, but, you know, just trying to improve the business process using technology. So then after that, you know, I went to college for four years. I was in what they call management information systems, which is kind of a blend of computer science and business administration. And after that, I just got an opportunity and my business started in 2005. So there was a guy that had kind of a small IT company and he was essentially just leaving. So, you know, I got a loan for $10,000 and opened my business. I would not recommend doing that, by the way.

Michelle: That had to be pretty scary. Wasn't it?

Marc: So don't open up with no customers, no cash flow or anything, and have $10,000 and try to make it work. But, you know, it's a you know, it's definitely a journey. But yeah, that was how I started. So it's 2022. So that's what, 15, 17 years now. And, you know, we're still trying to work on those same principles, right? So to use technology to make people's work flow better, I think a lot of people, you know, focus so much on just security or you have to get this. You know, the goal really now, especially with the labor Marcet the way it is, is like if you can't get new people, let's make the people that we have work as best as they possibly can.

Michelle: That's great. That's a great outlook. And I think a lot of small businesses really could use that within their business because we don't have a lot of resources. And so if you can use what you can that's available to you without taking up other types of resources, whether it's people's time, whether it's your time as the business owner or your money. If you can make things work a little smoother and still accomplish the same thing. That's good.

Marc: I mean, I always tell people, like, there are so many more things that are less expensive than people, you know.

Michelle: So, you know, now with technology, there's yeah, I mean, you can make that happen.

Marc: There's so many technology tools, so many things you can do to just make, you know, the existing people work better, faster, better, you know, more proficient however you want to say it. So you don't need, you know, you can wait, you know, a year or something to get that next person. If you can kind of just consolidate your time and do what you need to do and and get rid of as many, you know, mundane, you know, repetitive tasks, like anything you can automate, like you need to do it or make your, you know, just your your time more efficient when it comes to scheduling or whatever, you know, really work on those things before you're just like, well, I need to hire somebody to do this, you know?

Michelle: Yeah, I think a lot of people do that. Like we need another person. We need another person. And then all their overhead is like any extra money that they had is now spent out there. They're not really, you know.

Marc: Unless that person, you know, if you don't have 40 hours worth of work for that person, like you shouldn't be, you know, you shouldn't be hiring them because it'll just kill you, you know, if you try to grow too fast with, you know, ancillary people doing, you know, things because you don't want to do them, it doesn't, you know, it'll just. It'll kill the business quicker than anything else.

Michelle: Mm hmm.

Shawn: So many more applications and products speak to each other now than ever before. So you can. You can have these different things talking to each other and, you know, help eliminate some of that overkill with people.

Michelle: Mm hmm. Yeah.

Marc: You know, that's right. And we always tell people, like, before you buy a tool, make sure it fits like everything you want, you know, because there's tons of tools out there. You know, there's probably 50 different software companies that do one thing, you know, that you're looking for. So before you just go out, click the first Google ad and buy the thing, you know, that you find first, you know, make sure you find the one that works with all your stuff so that, you know, you're not putting your customer information into five different portals because none of them talk to each other. Mm hmm. Because that'll just, you know, it'll make your productivity even worse. Yeah.

Michelle: And it's confusing to deal with, like what do I have to update on this site and that site? Yeah. Yeah. Yeah.

Marc: Somebody gets a new phone number, they move, and now it takes you an hour to, you know.

Michelle: Then you need to hire an assistant to fix all these things. Yeah, exactly. Exactly. So you had quite a journey then. I mean, going from working for an insurance company and data entry kind of. Role. To run your own IT company with multiple employees, with lots of clients. And I think being that you're an asset in the small business, you are a small business. You can empathize with the small business owner for sure, and have a lot of value to offer them.

Marc: Yeah, I mean, we you know, I always kind of focus on what I call the VAC method. You know, when you're, especially when you're in a small business, you have to provide value, appreciation for your current customers, and communication is really critical, especially in our business. So, you know, in value doesn't mean like be cheap. It means that your customers need to perceive that what you're providing them is worth more than what they're paying you, regardless of the number. You know, it does it doesn't really matter what the number is, but if they perceive they're getting more value than what they're paying, you know, that will create, you know, that culture of, you know, raging fans where you're not only retaining your customers, but you're going to, you know, they're going to help you, you know, get more. And that's why we do a lot of appreciation, because I think one thing that, you know, people always hate the Comcast and Verizon method where, you know, let's give the new guy a better deal than you know, the guy who's been around for some years.

Marc: Yeah. Like people hate that, you know, and we try to not, you know, we use standard pricing that's tiered by employee count for every single per every single person pays the same amount of money and there's no deal for the new guy, you know. And if anything, some of our clients that are older, you know, maybe get a better deal than, you know, a brand new one. So I think you just have to, you know, make sure that your existing clients are, you know, know that you appreciate them. I think a lot of small businesses take their current client base for granted because they're like, well, I got them in and they're, you know, I think they're happy.

Michelle: They’re here and they're fine.

Marc: Yeah. You know, so just do a little, you know, send them a personal email like every once in a while. Just, hey, appreciate your, you know, you know, it doesn't need to be some grand gesture, you know, especially if you're in a business that, you know, isn't you know, we're in a business where, you know, our average client is worth a lot more money. But if you're doing you know, if you know you're doing pest control or something where, you know, it might be a one off transaction or something, but at least, you know, send a handwritten note or something, you know, people like that, those types of things. And, you know, it really goes a long way. We found we started doing like an appreciation campaign two years ago where we sent our clients kind of something, you know, every year with a, with a handwritten note that I wrote myself, which is it's grueling, but I think it's something that you, you know, it does make you the business owner really kind of, you know, make sure that you're touching base with your client base and stuff. But our referrals went up three x.

Michelle: Wow!

Marc: J ust by doing that, you know, once a year, you know, just sending them out to your existing client, say, hey, you know, we appreciate, you know, and there's no ask, you know, like, hey, we appreciate your business. That's it, you know?Don't try to cobble it together with selling him other stuff, you know, just, you know, make it, you know, kind of want to and then communicate. Like in our business, nobody communicates correctly. I would say the number one reason for our success is the ability to communicate, because so many IT companies, they're just they're either just trying to put the fear of God in people or they just they can't talk to human beings, which is kind of like an industry problem. I feel like.

Michelle: Yeah.

Marc: That I try to, you know, we try to get around, you know, but you know, just even if things aren't going perfectly with right now the labor shortages, supply chain issues like there's a lot of projects for in a lot of industries that don't go right, you know, yeah, whether it's construction or whatever. But if you can be ahead of it with the client and just kind of, you know, communicate like, hey, you know, it was supposed to be two weeks, it's going to be three weeks because, you know, we didn't get this part or whatever it, you know, people are willing to accept like those types of issues if you communicate and, you know, don't email them the day before, you're supposed to be there and be like, well, we're not going to be there because I never got the part two weeks ago, you know? That's a lack of communication. Yeah.

Michelle: Yeah.

Marc: S o it's really critical. They just make sure that you, you know, are in constant, you know, kind of back and forth with the client and just kind of keep them up to date on whatever is going on.

Shawn: Yeah. Yeah, we hear that a lot in a lot of different industries. And, you know, not just yours is, you know, the more you can communicate, the more you can be out in front of, you know, any problems or even good things. I mean, with, you know, letting people know what's happening, the better your relationship with those clients.

Marc: Yeah yeah. I mean and we see it, you know, right now, especially in our industry, the news cycle, you know, it's constant, like, oh my God, this happened or oh my God.

Michelle: Breaking news, everyday. Yeah.

Marc: So yeah, a pipeline gets hacked or this gets hacked or you know, there's all this stuff. So you just kind of, you know, we're kind of in an industry of, you know, everybody calm down, you know, like what we're doing, you know, this is why you're good. You know, here are the ten things that we're doing that help alleviate that problem and that kind of goes across the board for any industry. You know, when there's a news item like that that comes out, that happens, you know, for your business, you know, you kind of have to, you know, address it with your clients because you'd rather send an email to everybody than have your phone ring, you know, 30 times the next day with everybody just wanting a reassurance that they're okay.

Michelle: Yeah, yeah.

Marc: If you kind of get ahead of it, plus it, it reflects better on the company that you're not being reactive, you know, that you're being proactive to, hey, this, you know, this was out, you know, everybody's going to believe it's, you know, a big problem. So make sure that you're addressing it ahead of time. Not only makes you look better, but it helps, you know, calm your phone and your email box down.

Michelle: Mm hmm. Mm. Yeah, I understand that we deal with that a lot, especially in the last couple of years. With all the changes that we've experienced, it has been quite challenging. And the times have changed where, you know, years and years ago before us, people saw each other face to face so much more. And now we don't have that experience with each other. People are busy and they just don't have the time to come into our office or whatever. But, you know, communication is still very important in whichever way that people see to communicate. So I know there's so many clients that just want to use text messages. Yeah. And that's what's okay to say, hey, I was thinking of you, but maybe not so much for tax law changes though. Yes.

Marc: Yeah. You might hit a character limit.

Michelle: 20 text messages from your CPA. Not so good. But yeah, I mean it. Realistically, the idea is that we're just not in front of each other anymore. You know, as much as we used to be. So right. You have to.

Marc: You know, that you brought up. We do see that a lot now. And, you know, it's kind of like meeting people where they want to be, you know, because generationally we see a big difference as to how people communicate. Right. So some people still want to pick up the phone and talk to you. Some people would rather use email and, you know, some of the younger generation would rather text or you know, we have, you know, a chat feature on your website. Um, and I would say especially not so much for what we do, but if you're in any kind of emergency services, you know, like. If you're a pest control, plumber, like anything like that, where people are looking and they need that instant gratification of, I need this done, you know, like I want, I need somebody scheduled to come out. Like you need to make sure that you do all of that, that people can get in touch with you however they want, whenever they want. Because if you're not, the next guy is and he's going to be the one that gets the business.

Michelle: Understood Yeah, that's a great point. Thank you. So tell us a little bit about some of the things that you're seeing with IT and we had talked a little bit before we started the podcast about some things that people need to be aware of, especially on the IT side and cybersecurity. Tell us a little bit about your experiences with what's happening right now with some of this.

Marc: Sure. So we're kind of seeing a migration from, you know, where last year, in the year before, kind of the big, you know, story and worry was a lot of the ransomware stuff, which was all over the news then and than that hasn't that has not gone away. I don't want to say that it's gone away, but I think as an industry, we've gotten better at providing, you know, protections across the board that really mitigate that risk pretty good. But now we're kind of seeing what they call B.E.C attacks, business email compromise attacks, which where people are getting in the email addresses and kind of just parking themselves and waiting for an opportune moment to kind of get, you know, in between a transaction and really siphon a lot of money.

Michelle: Okay. So, I'm clear people are going into your email and they're not doing anything.

They're just waiting. Oh, wow.

Marc: Yeah. So just sit there and read it. And then what they do is, you know, once they see an opportunity, whether, you know, real estate transaction, you know, you're purchasing something or they they see where at some point somebody might be providing wire instructions for some reason, then they'll go create another email that might be a character off in the domain name from another person that you're communicating with. They'll copy their email signature and then they'll create a rule in your email. Basically any email from the correct guy goes to, you know, your junk folder or some folder that you're not going to see. And then they just start communicating as that person. And since they've been in your email, they know how that guy talks, they know what's going on with the transaction. So it seems very fluid. And then they'll just, you know, hey, here's the wiring transactions or, you know, whatever. And it's very complicated. And now there is, you know, there are some protections that you can put in place for things like that. But it becomes very hard for the user to kind of do, you know, it's a complex attack. So if you don't have certain things in place or if, you know, we really tell people when it comes to wire instructions, you have to be analog, there has to be an analog step, you know, where you're calling somebody on the phone or doing something completely outside of technology to verify that. And that should be a policy. And the company really has nothing to do with technology. It's just there needs to be an analog step if there's any sort of change to any financial, you know, whether it be a credit card number or whatever, that there be some sort of phone, and phone from the number you have on file, not the phone number, you know, that may be in that guy, you know, because there's so many way you don't email the guy, you know, and you know. So yeah, definitely analog methods for referring to, you know, wire instructions should be in everybody's policy.

Michelle: Yeah.

Marc: And if you can just get away from doing it completely, know obviously if you're in real estate or you know, there's obviously businesses that can't, but right. Your policies should have analog steps in them.

Michelle: Wow.

Marc: And you really need you should have somebody monitoring those logins. So if you're using like most of our clients are on Microsoft 365 so if you're using that, there's security services, you can get that monitor those logins to see if anybody else is in your account based on your IP address.

Michelle: Wow. So they can tell where that person's like potentially logging in. And then he says they know that that's not you or it's suspicious in some way.

Marc: Yeah. So they'll alert you like, hey, you know, log in from Taiwan or you know, and if you're on some of the premium services, you can actually lock those countries out. Just say, you know, we have a list of like ten countries that it's like no logging works, you know, it's just locked. You know, we don't allow log in from from certain countries. But, you know, there's a lot of things that small businesses can do that don't cost anything. They don't have to work with somebody turning on TFA on your email is like a no brainer.

Michelle: And just to explain what that is real quick.

Marc: Yeah. So two factors where you either get the text message on your phone or a phone call, or you set it up with an app on your phone where you got to put a code in. It's annoying and we know nobody likes it, but it's like the best thing you can do to stop those because it's so hard to get around it that, you know, a lot of people, you know, the business of cybersecurity is finding easy business, right? It's just like all of us are running. They're running a small business. So they're just trying to.

Michelle: It's just illegal.

Marc: Unfortunately, it's just a successful one. But they're looking for the easy ones. So if you have to offer on your account, they just go to the next guy because there's plenty of people out there that don't. So, you know, they'll just skip you, you know, unless you're like, you know, unless you have nuclear secrets or something where somebody is, you know, really targeting you. The majority of these attacks are people trying to get into a million accounts. They don't know who you are.

Michelle: They don't know who you are.

Marc: They don't know what your business is. They know how much revenue you have. So all these people are like, well, I'm too small. Nobody's going to target me. Like, nobody's targeting anybody, you know?

Michelle: Mass target, everybody's fair game. Yeah.

Marc: So, you know, if you think about it, a guy on the shore just casting a net, you know, whatever fish are in there is the ones he's going after, right? Yeah. So if you make your business like less of a soft target, then they just move on and pick the next easy guy.

Michelle: And so these are really I mean, getting a two factor authentication...

Marc: Authentication. Yep. Yeah.

Michelle: It's easy to turn on in the settings within whatever accounts. Yeah. Whatever in order to prevent, you know, someone just accessing it with a password I guess. Username and password.

Marc: Yeah.

Shawn: Are there any email services to avoid as a business?

Marc: Yeah. Anything free.

Michelle: There you go.

Marc: We go back to value, if you get a free email you're getting free value, you know, so you know, any of the carriers provided stuff, you know, Verizon, Comcast. You know, service of whatever Internet provider you have, don't get your email from them. Don't use free, you know gmail..

Michelle: Anything for the business. I mean, if you write for...

Marc: Personally, whatever.

Michelle: You can be exposed on the personal side with your personal accounts and things like that. Yeah, but sometimes people look at this in the business and because they're using or they house other people's information as well, they can't expose all their clients.

Marc: Yeah. What always gets me is, you know, I'd be very wary of real estate companies that use free email. You know, I see it all the time because, you know, agents are kind of, you know, they're subcontractors and they're just setting it up on their own. And, you know, it's a big problem because you figure out all the information that you're sending to a realtor for a closing a lot of times. And if they're on some free email service, you know, your stuff's just floating around on there waiting for something. And, you know, it's your Social Security, you know, whatever. And that's all just floating out there, you know, for it to be, you know, gobbled up and sold on the dark web for a dollar at some point in the future.

Michelle: Wow. So that leads me to I think one of the next things was about, you know, the dark web, right? So what you had mentioned that you had some things that people could do for themselves is yeah, you had said something about that to us earlier, but yeah. So you definitely want to.

Marc: You definitely want to go out and there's tons, you know, we have a service we use, there's tons of services out there that'll monitor your, you know, your company domain and even your personal, you know, you can even add your personal email to the Dark Web scans. And then what that will give you is if your password is leaked, right? So, you know, a couple of years ago, Target got hit. LinkedIn got hit a couple of years ago, Adobe got hit a couple of years ago. So and they'll tell you the password that's leaked and then you want to make sure you're not using that password anywhere that, you know, you really should make sure you're not using it at all anywhere now once it's leaked, but especially somewhere where it's meaningful, you know, bank, you know, credit card, you know, anything that has, you know, information that you wouldn't want to be public.

Michelle: Mm hmm. Mm hmm.

Marc: And that goes, you know, you can I we also recommend that people use a password management tool, you know, whether it be Dashling, Passfor there's a million them out there, LastPass, that enable you to create a complex password, you know, for, you know, every, every, every log-in you have you can have a unique password. And that really cuts down on that. If one of your passwords gets leaked, you know, it's just for that then particular vendor and you know what it is and you can go change it and make your life a lot easier than if your password gets leaked in an app is be your password for every login you've had since 1985, then it's a lot more work.

Michelle: With their email logins. Yeah. Yeah.

Marc: S o like that is, you know, that's the biggest thing. Like you don't want to make, you know, don't use one password for everything. It's just it won't end well, you know, somebody gets a hold of that. They now have access to your life.

Michelle: Wow. Yeah. So scary. I'm pretty afraid right now.

Marc: And those things are relatively, you know, they're relatively easy. You know, they're pretty easy to use. And, you know, 20, 30 bucks a year, we're not talking like some exponential, you know, investment to get into these things.

Michelle: Talk about value, though. That's probably a heavy value for it.

Marc: Yeah. I mean, they're so easy to configure. It's kind of like a no brainer. Like, I couldn't tell you what any of my passwords are. I don't even know what they are. You know, I think, you know, you go to the browser and you kind of hit the button and it auto populates your password from the thing. And, you know, you're, you're all good to go without even having to know, you know, what the password is.

Michelle: Wow. Wow. That's so good. Yeah. And then it just puts another layer of protection on you.

Marc: Sure.

Michelle: So tell us a little bit about some of the things that people are seeing. I mean, it all revolves around cybersecurity and being in business. How does that, you know, with insurances and things of that nature, what should be like, what is happening out there with insurances? And what are some of the hot points that people are having to deal with as small business owners in this area?

Marc: Sure. So we're you know, almost every day I get an email from somebody, you know, hey, we're trying to get cyber insurance. And here's a 50 question questionnaire you need to fill out for me. We definitely caution people like don't lie on those things, you know, be truthful. And if you are truthful and then they come back and. Say, Well, we can't insure you because you don't have this, this and this. Like, then you got to, you know, you make up your you know, you have to make up your mind because it's all risk mitigation. Right? So the insurance companies try to mitigate their risks. That's kind of our major business is risk mitigation, you know, for our clients is to take, you know, especially highly impactful events that have a higher probability of happening and let's mitigate those first and then work our way down. So those insurance companies that, you know, a lot of them now will ask you, do you have TwoFA on all your accounts? You know, so you need to make sure you have to make sure that it doesn't cost you anything. So make sure you're doing it. And I would say if you get that application and you don't know the answers and you don't you're not working with an IT company, you need to be. So if you can't answer those questions, you don't even know what the question is, then you need to be talking to somebody else, you know? I mean I mean, for years, you know, kind of companies have cobbled through, you know, a lot of smaller firms have cobbled through IT, you know, whether, you know, it's their brother's cousin or, you know, yes, I got a college kid who's really interested in IT like, you know, those types of things. It's too much risk to your business to not have a professional, you know, working on your stuff, because it's the one thing where you have to be 100% if you fail one time over 30 years, you know, that could be the time that you're out of business, you know, so, you know, you at least want to work with somebody. You know, we love everybody to work with us. But there's a ton of company. You know, there's a ton of managed service providers out there that, you know, you want to work with somebody that can answer those questions for you and walk you through. This is why you need this, because the insurance companies, now, they're making you prove it. You know, you can't just check all the boxes now and say, yeah, I have this, I have this. You know, they're going to ask either for proof from your outside vendor or proof internally that you have it. And some of them now once you get into higher value, they'll actually do testing to ensure that you do have it, you know, so if you say you have it.

Michelle: Even if you say yes and they'll come back and say, oh, we ran a test on you. Yeah.

Marc: And you don't.

Michelle: Not so much.

Marc: You know. I mean, it's the same thing. You know, you saw it in the credit card industry for years, you know, with the PCI compliance. At first it was a questionnaire and now they, you know, now they do scans on the network to say, hey, you know, you got the you know, these things in your firewall are right. You got to fix them. And we're seeing that across the board for almost every business. You know, it's more so we see a lot more of it in, you know, compliance industries, whether it's health care, you know, financial services, you know, if you fall under, you know, CMMC or any kind of compliance, you're going to have a much longer questionnaire. We see that health care can be like 30 pages.

Michelle: Well you're dealing with sensitive information, big time. And targeted too, yeah, they're targeted.

Marc: Yeah. I mean, because, you know, it's such a liability, you know, for you to leak one, you know, one Social Security number, one date of birth for, you know, one patient or something. And then that just becomes exponential if it's a large breach. So you really got it. You know, if you're looking to get and we tell people like you need to have cyber insurance and you're usually better off looking at a third party that just does cyber insurance. We found if you kind of compare the writers to stand alone, you know, writers on your regular liability insurance you can usually get more protection, more complete protection with a standalone policy than you will with just going on your regular.

Michelle: That's good information. I think a lot of people don't realize that, yeah. You know and you want.

Marc: And you want somebody in IT to explain to you what you're getting and what you're not getting because a lot of them, you know, they're going to give you, you know, 12 pages of what they're going to cover and what they're not going to cover. And you want somebody to be able to tell you, you know, what is the most likely thing to happen? And are you covered for the most likely thing you know? And where, you know, where is the problem going to be that's not covered?

Shawn: Or the most devastating, you know, the thing that would devastate your business the price making sure that that's.

Marc: Yeah. And that you have the right coverage you know because a lot of them they'll say, well, ransomware, we're going to give you 50 grand or, you know, for this, we're going to give you this much. And it's not. If you look at the failure rates, you know, one of the stats that we always use that's kind of really impactful is that 60% of businesses that experience a cyber attack are out of business within six months.

Michelle: Oh, wow.

Marc: It's not the initial attack. It's that now if you have a ransomware attack, it's not like getting, you know, dealing with the ransomware attack. It's now that your business doesn't operate for two weeks. You know, so, you know, people look at, well, 50 grand will be fine. And it's like, well, you got to pay your employees for two weeks. They're not working and you're not making any money. So you're going to need more than 50 grand, you know, like so.

Shawn: And are you really going to get all that data back that you lost? Right. Like, you know, you can even pay the ransomware and still not get everything back.

Marc: Right. And there's so many ancillary expenses. Right. So now if you leaked your customer data, now you need to communicate that leak to all those customers. And then how many of those customers are going to leave based on that leak? You know, so there's like all these things you have to consider when you're looking at, what am I insured for in one of my not insured for? It's not just covering the event, you know, it's covering, you know, what are the effects of that event going to be on my business after the fact?

Michelle: Oh, even scarier now. So. Yeah, so. Okay. So I think that what we kind of cover with some really good points that the small business owners can do themselves, but that really if you're running a business even just yourself, if you have highly sensitive information but you really need a professional in most cases, if you're if you're running a business, it's good protection. It's well, money your money spent well protecting yourself in that way and protecting your customers, clients or patients, for that matter. Sure. Yeah. I think the values there.

Marc: And I always tell people when you're in business, do what you're good at and let other people do what they're good at.

Michelle: Yeah, yeah, yeah. I am not IT. Yeah.

Marc: Yeah and I'm not an accountant, so.

Shawn: Yeah. We are big proponents of hiring the right people to do those things and, and focus on the things that you do best. Yeah, yeah, yeah.

Marc: Yeah. It's, you know, it's really critical to, you know, you don't want to cobble through things that are that critical to your business. You know, if something can completely ruin your business, you know, whether it's, you know, not having good financial reports so you can't sell your business or, you know, not having IT protection or, you know, not having somebody that's, you know, dealing with whatever, you know, you know, security inside your building or, you know, maintaining your fleet of vehicles like all those types of things. Like you need to find, you know, professionals to kind of deal with those things because if you don't, it just kind of becomes exponentially worse as the business grows.

Michelle: Yeah. Yeah. And it can't be managed. It's harder to manage and as you're growing as well, so. Sure. Well, thank you, Marc, so much for coming here and then talking to us today. We got to learn a little bit about your journey and how you ended up a small business owner and the people you see and help every day. And so we thank you for all that.

Marc: Thank you.

Michelle: Thanks, Marc. All right. Thank you.

Marc: Thanks.

Michelle: If you find this podcast helpful, then like subscribe and follow us on social media.