EPISODE 769

[INTRODUCTION]

[0:00:00.0] ANNOUNCER Welcome to the Real Estate Syndication Show. Whether you are a seasoned investor or building a new real estate business, this is the show for you. Whitney Sewell talks to top experts in the business. Our goal is to help you master real estate syndication.

And now your host, Whitney Sewell.

[INTERVIEW]

[0:00:24.4] WS: This is your daily real estate syndication show. I'm your host Whitney Sewell. Today, our guest is Brian Gill, thanks for being on the show Brian.

[0:00:32.8] BG: Thank you Whitney, it's a pleasure man.

[0:00:34.9] WS: Brian has been helping companies dig out of data related disasters for 20 years. He currently is the CEO of Gillware Data Recovery and is a cofounder of Tetra Defense. Tetra Defense is his businesses that are victims of ransomware and data breaches and provides ongoing IT risk mitigation. Brian, welcome to the show, grateful for your time. Though it's funny, we were just having some issues and Zoom was acting up in a big way for me and then we came back and it's working now and Brian said, "I think China or somebody is hacking you right now," and I said, "Well I know they're scared because I'm talking to you." Grateful for your time Brian.

In this business, we deal with so much crucial data, right? So much information that's very personal information for so many investors, it's so common for us to have a hundred to 150 investors in one deal.

[0:01:32.3] BG: Right, and you have all kinds of tax information and more than that, you're moving money around to the 150 people and your reputation means everything. When you're pulling a group of investors and you've got a reputation to success, you'd hate to see that reputation get flushed down the toilet because a bunch of wires went sideways or because you lost somebody's personal information to a hacker who steals their identity.

[0:02:00.4] WS: That's a hard conversation right there, I never want that to happen where I have to have that conversation with investor, give them a call to say I'm sorry I've lost all your information or I'm not sure if it works or not but you know, your money has, we don't know where your money is. Brian, that's horrible, right? Give us a little more about your background Brian, and what you do for people like us and let's jump in to some of those issues that we hope never happens and how you can help people like us to keep them from happening.

[0:02:31.4] BG: I was a computer scientist in about 20 years ago I started service company with some business partners called Gillware Data Recovery. What we do back in the day, what we did was primarily help small businesses out of normal traditional disasters, there was a flood in the data center, lightning strike and a server got smoked or a laptop or desktop got smoked and they didn't have adequate backups, they needed the data and then we have mechanical engineers, electrical engineers, people like that, tinkerers who would make temporary repairs to those devices, get people their own, reunite them with their data.

About six years ago, we started seeing this trickle of ransomware which is when a criminal syndicate or just a lone wolf bad guy hacks into a business network, encrypts all the data, steals all the data and then tries to monetize that event by essentially, all your data's encrypted, you got to pay them to get access to your own stuff and sometimes it is hey, if you don't pay me, I'm going to post all this stuff up to the web.

That just happened I think to a university in Nevada, just a couple of weeks ago where they decided not to pay a ransom and the bad guys basically released all the student's personal information, financial information. It's not just pay me for your own stuff, pay me or I'm going to blow up your business and blow up your reputation, right?

We started seeing a trickle about six years ago and it's been exponentially growing almost every quarter, we see about twice as much as the previous quarter and that has not stopped. About five years ago now, we started a company called Gillware Digital Forensics with a big intent on helping specifically do what's called incident response or cyber incident response, helping companies not just get the data but negotiate cryptocurrency deals with bad guys, perform the logistics, working with privacy councils on how they're going to disclose this to their clients, how they're going to disclose this to their employees.

If they're going to have to disclose this to some regulatory body, and then also solving the problem ongoing and providing risk consulting so not taking over their entire IT operations. But acting as essentially a third party watchdog to –

[0:04:57.6] WS: Nice.

[0:04:57.9] BG: Jump in once a month, making sure these businesses are doing the right things.

[0:05:02.1] WS: Yeah, well, I want to make sure we're doing the right thing, at least the listener knows as well, those that are operating this kind of business and have access to so much personal information for so many investors but also for the investor listening. It's just something to think about when you're transferring your information, transferring funds, you want to know that operator 's thinking through these things, right? You know, have some of these things in place.

[0:05:23.8] BG: Savvy consumers are going to be demanding that, they're going to want to know hey, show me your IT security, show me how you protect your data? The most savvy of these investors. Now, obviously, probably 80% of them aren't asking those questions but that's going to be a trend so you're going to need as a real estate syndication-type person, you're going to need to develop your response to this.

[0:05:48.5] WS: Okay, well you know, let's jump in there Brian, I don't even know where to start honestly. You know, we do some things but I just want you to walk us through a little bit, some things we need to be thinking about to protect that data and then let's jump in to – also, I'd love for us to touch on the wiring stuff as well, such an important part of our business but you know, think about the data, how do we protect that?

[0:06:10.7] BG: Yeah, I mean, it comes down to protecting your network, you know? Most of us are going to have either home network because of COVID. I'm at home right now. Or, they're going to have a small business network for their five or six employees in this, a lot of these big real estate companies were making these massive deals only have a dozen employees.

One of the biggest ones here in Dane County where I'm from is a family company of five or six people and they own hundred plus million dollars' worth of stuff, right? These are not large people-wise organizations. But they're very commonly targeted, this is the first thing to understand is the bad guys are freaking smart, they're really smart, they're not just smart with computers, they're trying to target companies that have weak IT and move lots of money around.

This is a prime target you guys, and that's a big problem. And we have a lot of clients in your vertical so what do we got to do? First thing we got to do. First thing we got to do is think hard about user authentication. How we log in to stuff, it is the year 2020, almost 2021 and if you are logging in to stuff with a username and password and that's it, and you got like three passwords that you use everywhere and it's like the name of your dog, the street you grew up on, you are going to get hacked, it is a guarantee.

You have to have two-factor authentication or even better, you can spend about 50 bucks, buy a little thing called Yubico key up on Amazon that will do basically a single sign on or what's called U2F or UFA which is essentially, it's replacing this whole password thing.

If you want to log in to stuff, you got to have this physical key.

[0:07:59.8] WS: What do you call that?

[0:08:01.7] BG: It's called a YuniKey, it's one vendor that I appreciate why YubiKey, I have no relationship with them at all, I'm not a paid sponsor or anything but the reason I like it is it's cheap. If you got five or six employees or two or three kids, you buy these things and when you go to sign up for websites and things, 80% are going to support these new security protocols and it's going to handle log in for you, it's actually pretty darn convenient and the only tradeoff is, don't lose your key, don't put it through the wash, put it on your actual keychain, that's what I do.

My keys are in my pocket, it's shaped like a key, it fits on a keychain and it works for your phone, works – I'm going to log in to something on my smartphone, it talks near field communication to my smartphone, logs me into everything, and if you don't have my key, you're not getting in. That's simple, there's no password to hack.

[0:08:59.4] WS: Nice. The problem then is not losing that key.

[0:09:03.0] BG: Right. My tools will back them up and you should be fine and if you don't have that, you're using username and passwords is fine but you have to use multifactor authentication, ideally like a rotating digit code, a lot of us are starting to see like the banks especially, when you go to log in to your bank, it's like okay, we're going to send you an SMS to verify that you're actually you. That's a second factor of authentication.

It's not a particularly good one, it's easier than you think, much easier than you think to basically spoof a sim and actually get access to those SMS's, and the worst method of multifactor is email. Yeah, I don't have my thing, email me for the second factor. We have to assume that your email got hacked, we have to think about these scenarios, okay?

If your email gets hacked, what do the bad guys going to be able to do? Again, to log in to your email, you got to have this multi factor authentication too and the biggest problem is the bad

guys are super smart and they might not try to ransomware you, they might say okay, I understand why I hacked this person in the first place, they're doing a bunch of major real estate deals, they're going to setup a bunch of email forwarding rules, every time you get an email from one of your clients, they're going to get CC'd on it.

As soon as they see the wire information start firing off, that's when they're going to hijack that communication. They might even send an email from you legitimately from you. That's the same email you were going to send them, are very similar, it's going to have a different wire.

[0:10:38.6] WS: Yeah, I've heard horror stories of this exact thing happening, you know, getting into someone's email, changing the wiring instructions that's being sent out and it's done before the operator even knows it.

[0:10:51.4] BG: Again, the good news there is the banking system's a little slow, right? It takes a few days for all those wires to clear. But the problem is, as your client is emailing you, first of all, you email the clients that got it, great, lovely. You know, we'll talk in a couple of weeks so you might not get a response but again, you might be like well jeez, why didn't they send the wire yet? You might try to send them an email and again, they're going to do what they can do to mitigate your ability to do that and they're going to try.

Again, when it comes to wires, you got to use the verbal, you got to verbally confirm these things, you've got to verbally confirm the banks and you got to ignore, again, ignore like the phone number that's in the email if you think that these bad guys are not capable of putting a bad phone number in there so that when you call to confirm everything that they're not talking, then again they might sound a little different but if you're putting together a deal 150 people and some of them you haven't met it's like, it may not work.

Again, with wires, try not to use email as the only way that you confirm the fact that you're writing around 10, 25, $50,000. Pick up the phone, hire an assistant.

[0:12:07.8] WS: Yeah, before we jump in to the wiring information stuff, I want to go back to just like the email and those things a little bit. I mean, obviously, most of our emails are Gmail, right? And it's not going to be that difficult for most people, especially like yourself, I mean, if you were that skilled at these things, to be able to get into a Gmail account or something like that and there are such crucial information there.

[0:12:29.9] BG: With Gmail especially, you can setup your Gmail to do multi factor authentication and you should. Again, Gmail fully supports all the new photo protocols that I was talking about so you can buy that UBI key, that's how you log in to your Gmail and when you do that, it actually becomes incredibly difficult for even a super skilled bad guy to penetrate that email.

Microsoft has similar things, you've got to setup something other than username and passwords for sure.

[0:13:02.7] WS: how does the system recognize that UBI key or computer or a phone, how does it know –

[0:13:08.2] BG: It's a little tiny thing that looks like a key, it actually has like a USB, it looks like a little USB stick, you can plug it in to your actual laptop or desktop and then when you go to login to something, you need to basically push the button on the key and then it will basically tell, it will tell that other service, hey, Whitney's logging in now.

They actually do – I don't want to talk about all the mechanics and all the – your audience doesn't care but it basically, if you don't have that key, you are not getting in and you have to physically have that key in your possession, you need to push the button, right?

With the cellphones, it talks near field communication, NFC and it's the same thing. When you're on the phone, I'm trying to log in to my Gmail, you push the button and it does that kind of wireless handshake.

[0:13:55.5] WS: Nice, okay. That's awesome. Well, one thing on that though, what about tools like LastPass or 1Password?

[0:14:02.5] BG: Yeah, those are good tools, they're going to make better passwords than you make, the problem is, if you have a weak password to protect your last pass then you're creating basically a single honey pot. If you're storing that honey pot up on the web, that's an incredibly bad idea in my opinion.

A lot of people host their last pass like up on a cloud service and that is an incredibly bad idea. You should have again, if I had to have one, you can have, there's another USB, there's a product called unicorn, it's a USB stick that has like a six – you can put a six digit physical password on it to unlock it, it's fully encrypted, you could put your last pass on something like that, even if you were like walking through the airport and dropped it, the bad guys are not going to get at it. But if you're going to have one of those, have an incredibly strong password to authenticate into the LastPass or the KeePass, they're certainly better at making passwords than you.

I prefer again the next generation of products to help with this is called, one of the vendors called YubiKey, that's just easier in my opinion.

[0:15:11.3] WS: Yeah, I'm definitely going to look them up personally. One thing though that's so helpful with something like LastPass or 1, some of those systems is being able to share a password while it's encrypted so you could share with a team member and they can actually see it. I can restrict access to certain platforms, do you have a way to do that?

[0:15:29.7] BG: Well yeah, there's a lot of different SSO or single sign on things and a lot of them have all these password sharing things and we just have to be very careful. As we dial up convenience sometimes, there's security tradeoffs and we just need to always make sure and this is tough, when you're like a real estate guy and maybe is like mid-60s, right?

You have to learn enough about the stuff to be dangerous you know? It's not everybody's favorite topic but you don't want to watch your whole business gets flushed down the toilet because you trusted some IT guy that didn't set things up right.

[0:16:06.4] WS: Okay, user authentication, that's great stuff. Anything on that before we moved to – as a wiring fraud?

[0:16:14.7] BG: Yeah, before we get there, again, I just want to spend like 30 seconds in a handful of topics, people can look this up on their own, you got to audit your backups so your backups, a lot of times, when we're talking especially to these small real estate companies, yeah, we got it backed up, we've got a USB plug that we plugged in and all the data go from here to there, that's not a backup, you're in the same network, you're in the same building, that's not a backup.

Your data need to get backed up to a completely different network and again, I'm talking about a cloud backup. If all your data is up in the cloud, you need to do a cloud to cloud backup. You need to have different networks, network segmentation. All good backup, assume that this network got hacked someday.

That's the mindset we have to develop is, let's assume this network got hacked, how safe are we going to be when that happens? How are we going to detect that, what is the worst-case scenario? If we don't want to get held ransom for our own data, it is simple. Have your data in an automated fashion, move to a completely different network with a completely different level of network authentication, IE, usernames and passwords, and again, there's got to be a multifactor authentication there.

Now we're making it exponentially harder for the bad guys, they can't just hack into one network, delete all the backups, encrypt all the primary and hold your ransom, right? The second thing is, you need to have a real big boy firewall, a lot of people, especially now, because of COVID are at home and they're literally just plugged into their cable modem. Doing 10-million-dollar real estate deals.

If this is you, you're a bad human, stop it, you got to stop it. You seriously got to stop it, you're just going to get completely crushed. You're funding terrorism, you got to really check yourself. You can't be doing 10 million dollar real estate deals, plugged into a cable modem people, you cannot do it. You got to have a real firewall and again, this does not have to be expensive, you know, there's a company called Eero, I think Amazon bought them, they make an excellent wireless mesh network for your house that's beautiful.

I love it, also, you can pay them a hundred bucks a year and that hardware appliance becomes a real big boy firewall and what that means is people can't just sit there and try to attack your computers because you have a firewall in front of that that's saying I don't know who you are Romanian IP address, go away.

They don't even get to that point where they're going to be trying to log in as you because you've got a firewall in between. That firewall, you guessed it, should have two-factor authentication, especially if you're like trying to RDP into your box and work without going through a firewall VPN that's going to do multi factor authentication, then we got a big problem and the last, so email security. Phishing is crazy, these people are smart. You think you're smart, you're too smart to fall for phishing you're wrong. They get everybody. So again, ego is a big problem with this kind of thing. People think, "Oh there is no way that can happen to me."

It could totally happen to you. The people that get crushed by this stuff are really smart. Really smart, really successful people and that's with phishing. So there is a service that I like. Well there is actually a bunch of different services that you can do. There is a service that I like called Iron Scales, it is pretty inexpensive. Buy if from your MSP. It is basically like a crowdsourced phishing email scanner. So as a whole bunch of other people flag these email addresses as kind of bad.

Or these messages as fraudulent of fishing, they will essentially never show up in your inbox to begin with. So that is a product called Iron Scales I really like for email security. I guess the very last thing is you don't let your kid's log on to your work computer and install a bunch of

weird software. It sounds simple but sometimes you know we have a laptop and your kid wants to jump on and they want to download some weird program or something.

And it very well could have some backdoors and phishing and even things like TikTok. People are saying, "Oh there is a lot of security concerns that the US government had about TikTok because there's all kinds of weird stuff that that tool is doing," and nobody quite understands why and that's a really big example of it but it wouldn't take much to make some little kid's program and have it be free and then you install it in your computer and push the button that says, "Yep, install this software please it's fine."

And then, oh by the way, it is scanning your hard drive and shipping your stuff off to Bangladesh. Don't let anybody use your work computer.

[0:20:59.6] WS: You know I was just trying to sign up for this thing the other day that somebody invited me to. I thought it seemed like a great way to meet new investors and whatnot and through the process it says you are giving access to this program to all of you – I mean it says, you're giving permission for them to copy all of your contacts, all of their addresses. It tells you this, all of their addresses, their phone numbers and it says like any information about that it just lays it out there and I'm like, "Uh no, I don't think so" you know? And I don't think so, you are not going to do that.

[0:21:36.5] BG: They don't always warn you especially if the software was designed to steal without telling you. They are definitely not going to warn you on that. So you know again, I find it is just easy especially because so many of us are working from home and you know the kids want to jump on and they see you doing stuff on your computer and it's like, "Yeah what is the harm?" like no, this is daddy's work computer. No you can't install your weird software packages on it.

[0:22:00.9] WS: Yeah. What about when you are talking earlier about cloud backup, what's your recommendation there? You know most of us are probably using Google, right? Google Cloud or whatever, is that a big no-no?

[0:22:13.9] BG: Google is a good company, right? You know our alphabet is known now. There is definitely a handful of cloud service providers that are very well known and very well secured but you have to turn the security on. That is where we see most of the problems like AWS is amazing. You can configure AWS a million different ways for security but if you don't take advantage of those things then it doesn't really matter.

It is more about the human that's configuring it than it is about the provider and you know especially as a small real estate business, you should not be doing this yourself. You should be hiring a manager service provider with a security pedigree and they're not going to be the cheapest one in town. If you pick your MSP because they have the cheapest rates and you bring them in when the world burns down exclusively, well then you are doing it wrong.

You need to pay them a small amount of money every month to manage your security and your systems. As far as backups go and again, this is not the kind of thing that if I am a real estate mogul, I am going to be doing but you know most of us are on prem, or servers or cloud servers are running virtual these days. There is a great company called Veeam that makes an amazing backup utility and then you could configure it to push to something like AWS.

There is another wonderful company called Storage Craft out of Draper, Utah that makes some really excellent backup stuff as well but again, it is not as much about the provider as it is about the human setting it up.

[0:23:50.4] WS: Okay, no that's awesome. We are about out of time Brian. This is some such good information but I want you to be able to elaborate on wiring fraud and as operators how we can take steps to prevent that.

[0:24:05.7] BG: Yeah. So it just you know we got to double, triple, quadruple check these things and you got to add whatever efficiency that you had by just sending a 150 emails saying, "Please wire these over here" we need to shred some of that efficiency. We need to get more inefficient. We need to take our time here. We need to verbally tell our clients like I will

never email you telling you – "I will never email you exclusively telling you to wire money somewhere."

Just tell them that. I am always going to have me or one of my staff call you to do a verbal verification, always because and again, we just went from a negative to a positive. You might have trust that they're going to have and you just went up, right? Because you're telling them I don't exclusively trust email because I have an obligation to protect your money and make sure that it gets into this real estate project, right?

We want to make sure that we are familiar with the banks that your clients, they know how to verify that it's real. We got to slow down is the biggest thing and again, most of the problems can be prevented by having dramatically increased email security, dramatically increased user authentication. Most of these hacks start with email. So don't overly rely on email and lockdown how you and your staff login to email and again, I would the pros –

One of the other crazy things and again, I don't want to go way too far down the rabbit whole but if you had whitneysewellrealestate.com and you're emailing your clients from that, it is so simple to set up a very similar domain with real estate with the letter three backwards or something, right? And be emailing people. So don't put your client's information anywhere on the web. Don't put any of your high net worth clients or partnerships on your website.

You know be pretty smart about it all and LinkedIn is another one. A lot of you folks are using LinkedIn quite a bit to communicate and use the LinkedIn messenger, things like that. You got to multi factor in your LinkedIn, you got to be suspicious about LinkedIn. You know again, my biggest advice is to slow down.

[0:26:35.9] WS: That's awesome. So important, man so important especially the wiring stuff. I love just how you talk about slow down convenience really causes problems a lot of times and thinking about how to be more convenient as oppose to taking those extra steps. I know even that phone call letting investor know that someone from the team is going to call you to verify the wiring instructions before you send a wire, right?

You know if we are doing that, could we email it to them right then and say even when we're on the phone and say, "We are just verifying that you received the correct wiring instructions before we do this" or something?

[0:27:10.5] BG: Yeah and again, you might even consider moving to a securebox.net account or a secure file sharing app instead of an email attachment because again, one of the problems of email is that information can usually just sit in your inbox or sit in your archive for seven years. It might be a better way to actually have like a secure file sharing.

[0:27:37.0] WS: Yes and you said that's securebox.net?

[0:27:39.4] BG: Well that is one of them and there's a million of them I mean and again but this is the kind of thing I'd be relying on my MSP for. How can I securely share these wiring instructions with my client? And the more we can get away from email, the better because it really is when we investigate all of these breaches and all of these hacks and all of these data thefts and all of these ransom ware events, probably my rough guess is 75% of them originate with email. We got to be really, really cognizant and not using it when we can.

[0:28:12.5] WS: Awesome Brian, well unfortunately, we are running way low on time and maybe we probably have to have you back sometime in the near future so we can dive into some more of these things. It is such an important topic but a few more questions quickly Brian. You know I believe every entrepreneur or business owner has to have a high level of self-discipline to be successful and how have you gained that high level of self-discipline?

[0:28:35.3] BG: Yeah, I mean it just think it comes from knowing how many hours there are in the day especially when we got our families running around as we get older. We have to wake up every day with a certain amount of intent thinking about what we are going to have accomplished and holding our self accountable to accomplish those one or two or three things and not have it be 17. You know for me, I'd really had to learn how to say no.

And I had to learn how to delegate because if I wake up with 17 things to accomplish, it is just not going to get done. It is going to grow and grow and grow and then I am going to be buried under a mountain of my own tasks. You know, you've got to – what am I doing today? One, two, three or four things that's it. Don't go to bed until they're done. Just behaving that way you can develop that discipline at least that is how I did it.

[0:29:29.1] WS: I like that when you said we have to wake up every day with a certain level of intent. I like that. What are a couple of habits that you have that you're disciplined about doing, say on a daily basis that have helped you achieve success?

[0:29:42.4] BG: Yeah, I mean I just used again my Outlook Calendar, right? I have scheduled one on ones or small team meetings with my team and they start on time, they end on time. We do them at least once a week. Those times are blocked off and the phone is off and kids are doing something and like I always am going to have that time with my teams, right? And so much of my success and I imagine it is similar in your world it comes from team building.

Hiring the right people, meeting the right people, treating them well, maintaining those relationships. If you don't start with the right team and if you don't – some of the negative things about running businesses and doing deals is you got to cut people out sometimes that are not the right kind of people and that can be painful but your job as the person in charge of the organization or in charge of the deals to determine who is going to be members of the tribe here, right? And if you are not going to do it, who's going to? So sometimes that means making some hard decisions.

[0:30:52.6] WS: What's a way you've recently improved your business that we could apply to ours?

[0:30:56.7] BG: Maybe it is not as far as the business goes because again, some of these crazy stuff that just popped into my head is no applicability to your world but as I get older, as I get more success, I keep slowing down. We'll go back to it you know and just thinking about, "Okay, this guy" whether it is an employee or client they want us to do a certain project or one

of my employees wants us to do a certain project and not always saying, “Yeah, let’s go do that.”

But really just being like, “Really? Why should we do that?” and then at the end of that half hour, maybe we still are going to go do that but not bought in, right? And maybe I’ve shot some holes in it. That person is going to go back and do their homework and come back with something a little better and you know back in the day especially when I was in my 20s and running around and kind of a more tech startup mode and somebody had an idea that’s like, “Do that and do that and do that and do that.”

And again, we had a lot of success. We also had probably too many failures too. You don’t want every deal. You don’t want every investor. Slow down.

[0:32:09.9] WS: Love that, yeah great answer Brian. Tell me the number one thing that’s contributed to your success?

[0:32:15.7] BG: Knowing myself what my strengths are, what my weaknesses are, what I’m good at and again, I’ve had and especially in my youth I had maybe an overly healthy ego but not becoming cocky, you know being confident but understanding what I do and what my company does and our role in assisting our clients, it just helps make all of the other decisions so much easier. The more you understand what your role in all of this is.

You know you don’t need to threat overall these things because you’re so confident in your role in society, your role in the company, your role in the micro verse. So when it comes to all of these 15 different decisions we got to make every day, it just becomes so much easier. Like in the early days, you know when you don’t really have that confidence, when this is all just an idea this whole like, “We save data for people and help businesses out of data disasters.”

This was in the ether 21 years ago, right? I mean it is hard to have that confidence when you are in that ether and you’ve helped nobody. 21 years ago I helped nobody and it’s hard to have

that confidence and know your own universe because it is just a concept. So you know, you got to have some amount of success to have it snowball.

[0:33:39.9] WS: And commitment in the beginning, no doubt.

[0:33:42.8] BG: Oh, a lot of long hours, you got to make up for all of those mistakes you are going to make.

[0:33:47.2] WS: How do you like to give back?

[0:33:48.7] BG: Yeah, I mean I like youth, I coach a lot of youth sports with my son when I can. I've been on a handful of non-profit boards my wife and I. My wife is a doctor at a children's hospital here. We like to attend and go to a lot of various fund raisers and fund raising activities for the children's hospital. I mean you can't really pick a better charity than sick children and some of the stuff that the pediatric community sees just no matter how bad my day is, nobody died you know? Some of the stuff that they see just will break your heart. I like to support my wife in her endeavors.

[0:34:33.4] WS: Nice, no I love that. That's awesome Brian. I appreciate you giving back in that way and great show. Man, I am just so grateful to have met you personally and just the listeners can meet you as well and realize how big a risk their data is at and there is all the investor information and personal information to their funds, you know doing a wire transfers and you just exposed a lot of that I think to listeners and myself and tell them how they can get in touch with you and learn more about this?

[0:35:02.1] BG: Yeah, so a couple of resources. I have an MSP buyer's guide on gillware.com. It is not gated so if you just Google for Gill Ware or MSP or manage service provider buyer's guide. We put together a list of 30-ish questions that you can interview your MSP because that's a problem, your real estate guy you got to hire an IT guy, you have no idea what you're doing.

[0:35:24.1] WS: Tell us what MSP is again?

[0:35:26.3] BG: Manage service provider. So again, most Americans work at companies of less than 50 employees most of us and all of us need IT help. None of us can afford to have a full-time employee as an IT guy. So there is the concept is manage service provider. There is probably 20,000 of them in the US that provide the IT. It's like a time share on an IT guy. You pay him a thousand bucks a month, you get a quarter of an IT guy.

But then they are also if their good ones are helping you with your security decisions, helping you with your file sharing decisions, helping you with your backups, helping you audit those backups, helping you with your authentication do hickeys.

[0:36:08.3] WS: Nice. So how can they get in touch with you?

[0:36:10.4] BG: So again, if you Google, I am on LinkedIn. So just Brian Gill, Gill Ware on LinkedIn, I'll pop right up. You can connect with me. The MSP buyers guide is up on gillware.com. It is not gated, just Google it, download it, use it. There is also a thing up on Gill Ware, it's like the seven things you can do right now and within two hours to dramatically improve your security. So there's a couple of free resources up there you can Google for.

If you want to connect with me personally, it is Brian Gill from Gill Ware, just Google that and I'll pop right up on LinkedIn.

[0:36:38.8] WS: Awesome Brian, great show. That's a wrap, thank you very much.

[0:36:43.0] BG: Thanks man, it was a lot of fun.

[END OF INTERVIEW]

[0:36:46.0] WS: Don't go yet, thank you for listening to today's episode. I would love it if you would go to iTunes right now and leave a rating and written review. I want to hear your

feedback. It makes a big difference in getting the podcast out there. You can also go to the Real Estate Syndication Show on Facebook so you can connect with me and we can also receive feedback and your questions there that you want me to answer on the show.

Subscribe too so you can get the latest episodes. Lastly, I want to keep you updated so head over to LifeBridgeCapital.com and sign up for the newsletter. If you are interested in partnering with me, sign up on the contact us page so you can talk to me directly. Have a blessed day and I will talk to you tomorrow.

[OUTRO]

[0:37:26.3] ANNOUNCER: Thank you for listening to the Real Estate Syndication Show, brought to you by Life Bridge Capital. Life Bridge Capital works with investors nationwide to invest in real estate while also donating 50% of its profits to assist parents who are committing to adoption. Life Bridge Capital, making a difference one investor and one child at a time. Connect online at www.LifeBridgeCapital.com for free material and videos to further your success.

[END]