PODCAST TRANSCRIPT

Cybersecurity for Family Offices: Protecting Wealth in the Digital Age

Season 01 | Episode 10

Mark Wickersham (00:55):
Alright, welcome to the Risk Clarity Wealth Tech podcast. Today's show is about cybersecurity and what family offices can do to better protect themselves. I got a couple great guests today. I have Tony Ghibli from Anna Cybersecurity and our very own Carl Connect CTO and President of Risk Clarity. How are you guys? Great. How about you? Doing well. Let's do some introductions First, Tony, why don't you give a quick introduction and then Carl, and then we'll kind of get into the questions.

Tony Gebely (01:30):
Sure thing. Yeah. I'm Tony Gebely, CEO and founder of Enterprise Cybersecurity. We help families develop cybersecurity programs and we only work with families and family offices.

Carl Knecht (01:43):
Hi, I'm Carl Connect, president and CTO of Risk Clarity. We provide myriad of services for ultra high net worth families and those who serve them, specifically financial technology integration, back office reporting. I've been in the industry for most of my career. I've worked with single family offices, multifamily offices, wealth managers, RIAs really on the technology side development as well as providing technology services.

Mark Wickersham (02:16):
Great. So Tony, always love a chance when I get a chance to talk to a founder, would love to hear your founder story. Why did you start the firm? What was the need in the marketplace that you saw? And then kind of taking a look back on your experience, what surprised you the most?

Tony Gebely (02:37):
Yeah, sure. Been in it all my life. I mean, I was programming when I was 10 on our 4 86 in our family room. I mean, I've always been interested in computers. I've always been a nerd and went to school for Compsci at Rowan University in New Jersey and then just launched my career after that and worked for various startups, some in the Chicago region and then found my way to a firm called Family Office Exchange in Chicago. Before I worked for that firm, I didn't even know what a family office was and I was leading their technology practice and after a while I was with the firm for 12 years. After a while I just started to talk to members about cybersecurity and I became the subject matter expert for cybersecurity and directly work with some families during my time there and help them, help push them in the right direction with cyber.

(03:28):
But really the way I went from not understanding how families should handle cybersecurity to having a keen understanding of it and getting that experience during my time at Family Office Exchange is I was learning from the members. There were several members there that were really handling this topic well, and some of them had directors of family security that oversaw all aspects of security. And what they were telling me was that you cannot approach security in an ad hoc manner because you're only as secure as your weakest link. And that principle just really stuck in my head, okay, you're only as secure as your weakest link. So how do you go about cybersecurity? That means that finding a list of 10 best practices, while it can increase your cybersecurity posture, how does it know where my weak links are? And so the members that I worked with that I felt were doing it right, they started with assessments and the assessment was a mechanism to uncover the family's weak links.

(04:35):
And during my time there I started to parrot that advice back to members that I didn't feel were handling cybersecurity in a way that was praisable in any way, shape or form. And they were receptive because it's a really confusing topic. A lot of families just step back and family offices will step back and just like, I don't even know how to approach this. It just feels like too big of a problem for us. Too expensive to combat and cover all of our bases. But when you say to someone, just start with an assessment and just drop the mic, that's it. Just start with an assessment that will uncover and prioritize your weak links, what you need to spend money to remediate. And that's what ultimately led to me leaving Family Office Exchange and starting my firm was the fact that I didn't see any other providers in the space that were doing comprehensive threat assessments across everything a family owns, not just their business and their family office, but their homes, aircraft, yachts, vehicles, anything that connects to the internet should be part of this threat assessment.

(05:48):
So that's really what led to it. The other thing that I'd be remiss to not say this was I saw that there were software platforms and network monitoring platforms that were going after family offices and saying, buy our software, throw our network monitoring device on your network and you'll be secure. And that is just pure snake oil. Some families were like, okay, great, we checked that box. Cybersecurity's a box, we need to check. They feel good because they did something. But what about education? There's so many other facets to the cybersecurity issue that cannot be solved with just a piece of software. If someone, social engineers, one of your staff members, and because they were uneducated and didn't know how to spot a social engineering attempt, what software platforms going to stop that from happening? So that's what really emboldened me when I saw these other successful platforms selling to the family office space and thinking that they were making them secure. I mean, sure, maybe some of these platforms are part of a comprehensive cybersecurity program, but they are not comprehensive in nature and that's ultimately what led me to start this firm three years ago.

Mark Wickersham (07:06):
So would it be fair to say that an assessment basically creates a roadmap for these families and family offices and kind of details out where they're doing good, but more importantly where they need to shore up?

Tony Gebely (07:20):
Yeah, that's exactly, it provides a roadmap. It's a prioritized view of risk, and it doesn't have to be prescriptive in nature. I mean, the way we do it is we sit down with a family or family office executives and we'll go through each risk that we found and our recommendation and they might be like, well, that's too costly for the risk and they weigh the risk. Everybody has a different risk appetite and we end up collaboratively designing that roadmap. I mean, our recommendations that come out of the assessment are one thing, but what actually gets implemented is a collaborative process between either family members themselves or family members, executives and my team

Mark Wickersham (08:01):
Bringing in Carl and talk a little bit because on the vendor side it's a little bit different, but I'm a lot of principals still are the same. What should family offices be thinking about when it comes to vendor management?

Carl Knecht (08:15):
Well, I think starting with what Tony said of a baseline assessment, where are you, what are your pieces? And a lot of times just figuring out what you have in place, whether that's vendors, hardware, software, employees, staff, other third parties, having that baseline, you'd be surprised how many vendors, families, family offices, any business has started to amass over time, especially if they're coming in with no baseline and really no security in place. You have staff, oh, let's try this. Or a family member especially, I want to try this new software that just came out, this SaaS product, and you try it once and forget about it and you move on.

(09:03):
So the vendor assessment really starts with that baseline. What are the vendors that you're using? What are those third parties that are in place? And really asking a lot of questions of what else have you tried or searching through what other logins the users, the family members might have and start pulling a thread and working through where else are they? Is this data really been moved to or where's the family information that's stored? So really just starting with a real basic, what vendors are in place, what third parties, and really what we're trying to get at and the families are looking for is where is this family information? Where's this data? Where has been shared and how do we start to assess those vendors and the security in place on those vendors? We've definitely seen, and we're more on the supply side since we're providing software and we're providing services to families and multifamily offices.

(10:07):
So we're constantly reviewing our vendors on behalf of our clients as well. So they're looking to us as a vendor and they're starting to look at who our vendors are and ask questions, how do we manage our vendors? So these are even the questions that the

next steps of, once you know who your vendors are, start asking the vendors questions. And I know Tony has a great process around working through this baseline, but then looking at each vendor and having a process and having procedures in place for reviewing your vendors, tracking your vendors and regularly assessing them, whether that's bringing in another party to help assess those, but at least keeping track of who they are, keeping track of your contracts, keeping track of all the information around them, and it can be a daunting task.

Mark Wickersham (11:00):
Yeah, it does seem there's a lot more emphasis on third party risks, which is great. I mean, that's the next level. These firms are not only getting a handle on their immediate risk, but also is taking a look at it as to your point, who are the vendors my vendors are using and do I have any concerns in that area? Are they on top of their particular vendors? Tony, when you're working with family offices on vendor assessments, tell me a little bit, especially around the vendor selection and evaluation process, what do you look for? Tech vendors?

Tony Gebely (11:37):
Yeah. Well typically inventory all the vendors of families using and then classify them by what sort of access they have to the family's information. So if a handful of vendors have access to financial information, we'll start there and start asking them questions. And if it's a major multinational bank, we could make certain assumptions, but we still have the conversations. If it's a local family office service provider, we'll dig a little deeper and start with some really easy high level questions and just look for some red flags. One example, I was helping a family evaluate an MFO and I spoke to the president of this M ffo and he said, oh, we're probably going to have multifactor authentication enabled for all of our staff by the end of 2024. This is in January, and that's all the red flags. I need to go back to the family and say, whoa, hold on.

(12:38):
What we do look for shops that have their act together usually have a security one pager. They get assessed themselves. They might even share with you the result of their assessment. That's the gold standard. Like, oh yeah, we get assessed every other year against the NIST cybersecurity framework. Here's our most recent version of the assessment. It might even be on an online platform and they just invite you to it and you just go through it and look at how they fared. I mean, that's best case scenario. Few and far between though, to be honest with you, which is absolutely crazy in this world. But yeah, it all starts with classifying them based on what level of access they have to the family data and then just going through basically a subset of the assessment that we would've done for the family themselves. But large firms are used to this. This is just par for the course for enterprises. You could go to a sage intact or something or a major platform like that. They're going to have an individual that just responds to questionnaires all day because they get it a lot for this vendor. Due diligence process,

Mark Wickersham (13:43):
Family offices obviously are targets for cyber criminals just due to the nature of the relationship with the families of significant wealth. I think there's a recent Deloitte

survey that said four in 10 family offices had been received a cyber attack within the past 24 months. I assume these numbers are probably lightly reported. That number could be higher considering that some may not be reporting. Denton's also had another survey that came out, a risk management survey that three in 10 a family offices said they had a robust family cybersecurity program in place. What is some of the biggest mistakes that family offices are making? Tony, we'll start with you and then Carl, we'll look for you to bring us home on this one.

Tony Gebely (14:34):
Yeah, I would say so. The biggest mistake that we see in the field are families that think that their IT staff is handling cybersecurity and especially families that just have one IT resource on staff, like a full-time employee. Oh yeah, John, he handles our cybersecurity and

Mark Wickersham (14:55):
Cyber is like one of many things he does.

Tony Gebely (14:58):
Yeah, you really need that third party view. It doesn't have to be us work with, there are a number of companies out there that do this sort of assessment service. So just have a third party look at who you're using. Even if you've had this guy on staff for 20 years, or even if you're using an MSBA managed service provider IT firm, they still need a third party assessment from time to time to keep them in line and make sure that they're keeping up with the cybersecurity standards. The other thing that I see a lot is this won't happen to me. We're a private family. It could happen to your vendors, it could happen to a software vendor. It doesn't have to be like a law firm or your accountant or your RIA. It could be a piece of software you use that you trust with your data.

(15:43):
So having that full cybersecurity program that includes a vendor risk management program, you don't have to manage it yourself. You can get a cybersecurity firm to do periodic assessments of your vendors for you, so you don't have to worry about taking on that burden. But I would say the top two mistakes are assuming that it handles it and having it. It can't happen to me attitude because a lot of families, once it does happen, that's when they start to build their cybersecurity posture for the next time it happens. But if you handle the proactive cybersecurity before an incident occurs, then you're, you're ahead of the game

Carl Knecht (16:17):
As so mentioned when we're talking about families not thinking that they're a target or that they're going to be hacked or addressed or really they keep a low profile. However, I've seen areas especially where there's mass viruses or mass changes that are out that happened to come across a staff member. So I think there's an incident or ongoing issue with Word documents. Family offices transfer money all the time, a lot of transfer documents, a lot of transfer information, and there's an issue with a virus in Word where bank account numbers are getting changed. So say a bank account number is changed in a Word document, that document gets sent to a bank for a

transfer, the number looks fine, both parties agree that's the same account number, and now money's being transferred when they don't expect it to. So the thought that they're not a target or that they keep a low profile, they can get caught up in these transfer schemes and it can be hard to find. It can be hard to track down. So not having the processes in place, not having the process with the family members, and I think this is getting a lot better in place. So not having those processes in place of typical transfer or other types of following the money or following the process. So there's always double checks, there's always verifications, whether it's with transfers or any other type of management.

Tony Gebely (17:48):
Carl, you touched on something really interesting there, the fact that a cybersecurity cyber attack could be non-targeted, right? So I want to dig into that just for a second here. So there are primarily two types of cyber incidents or cyber attacks. One is targeted. The bad actor knows who you are. They know that you're a person of wealth or that you manage money on someone's behalf. That person, if they know who you are, will find a way in. They're going to know where you live, they're going to look at open source intelligence information on the web. They're going to find a way, and that's what you need to be worried about on one hand. On the other hand, the folks that think that they're not a target to address that, the other type of attack is what I would just call a random numbers game sort of attack, where a bad actor will build a bot that just scans the internet for vulnerable machines that are exposed to the internet. And when I say vulnerable, I mean something that hasn't been recently updated and a vulnerability hasn't been patched. Those types of attacks are actually way more common and can impact anyone that's connected to the internet that has a vulnerable machine, browser, phone, whatever, as long as it's out of date, meaning that you haven't been keeping up with your security patches or your IT team hasn't been keeping up, you're subject to random attacks. So that just goes to show anybody is vulnerable in this day and age.

Mark Wickersham (19:20):
So Tony, obviously you're a big proponent of the threat assessment. Can we dig into that a little bit? What are some of the key pillars of a threat assessment? What should a threat assessment cover? How often should a family office do one? What should they do with it? Tell me about how important tool is and how you form one. Yeah,

Tony Gebely (19:40):
Absolutely. So a common misconception is that a threat assessment is all technical in nature, but that's not true. Most threat assessments, well, all threat assessments should be based upon a cybersecurity framework. And there are several out there that are just open free to everyone on the web. The NIST cybersecurity framework is one of them. ISO puts one out called ISO 27,001, but that's more for manufacturing firms. And the Center for Internet Security puts one out. And these are basically giant checklists of like 150 things that every business should be doing to keep up with cyber attacks. And each one of them go into, obviously there's things in there like network infrastructure, proper configuration of devices and network devices, keeping things up to date, like I mentioned earlier, proper tooling like for monitoring, for

scanning, use of next generation antivirus such as EDR, use of password management tools, but also these frameworks touch on education programs.

(20:45):
Are you educating everybody and are you teaching them the things that they should be learning? Are you doing social engineering tests, IE phishing your own employees? Do you have the correct policies and procedures in place to protect the family's assets? And that's anything from having an incident response plan, a business continuity plan to, on the procedure side, having a process in place to double check account numbers before you transfer money. So a proper threat assessment should look at all of those things. So when you're out there in the market shopping for a firm that does this sort of thing, make sure that they're rooted in a well-known cybersecurity framework, just know enough to be dangerous. Just ask them, are you using CIS? Are you using nist, iso, whatever, but also ask them if they're doing things on top of that, because I mentioned earlier that these frameworks are built around businesses and family offices, protect families and homes and personal devices and non-business type things, right?

(21:53):
So any sort of assessment firm that you work with should have experience working with families and go above and beyond the business-centric frameworks to look at things that would kind of just skirt right in under the rug when you're doing a business-centric assessment. One example I'll give you is that these assessments, because they're about assessing businesses, these frameworks, they're just for businesses. They assume that everyone is using a business email account, but we all have worked with family offices wherein the family members all have personal email accounts and the family office is sending investment reports, et cetera, to a Hotmail, Gmail, Yahoo that will just skirt right by an assessment because the assessment assumes that everyone in the quote business is using business email. So that's just one example of how they should be rooted in a cybersecurity framework that you at least have some sort of knowledge about, but they should go further if you're looking at protecting the entire family and their assets.

Carl Knecht (22:58):
Tony, a question on that. As far as the unique assessment that needs to be done for family offices now, they also have potentially outside businesses, other email addresses, like you said, other information as well as internally within the families segmentation within the family office. As far as information security between maybe groups or family members. How do you approach those unique variable or business security issues as well?

Tony Gebely (23:34):
Yeah, typically we'll get the family on a family office domain email account, and if they're using Microsoft 365 for that, we can segment access to files using SharePoint. If not, we can use something like Sumita or maybe even like a trusted family platform wherein you can create different family groups and share assets with them in that way. But definitely not just over email as attachments, right? The second you send an attachment outside of your domain, you have no control over it. So data governance

is of key concern with this topic, making sure that you control your data and share with the right people using the right tools.

Carl Knecht (24:17):
For us as a business. We have policies, procedures, documentation. Do you find that many family offices have any documentation when you start with the assessment and how far do you go working with them on documentation and policies and procedures?

Tony Gebely (24:34):
I would say half of the families we work with have a written information security program that includes some form of incident response process, but we work with them to, if a family doesn't have this, we have templates that we've developed that we'll tailor to the family, and then each year we'll do a review to add things to it. One popular thing that we were adding to written information security programs last year was policy around ai, use of AI in the family office, specifically around not putting personal information about the family into something like a chat GPT, which could possibly use that data to teach the model. So a lot of the, it's really difficult to tell the staff don't use it at all, but we can build some policy around it and say maybe obscure names, just generalize it somehow, make it the Smith family every time you type out the family name or something into chat, GPT, those sorts of things we add into policy. So we'll typically do a review every year of a written information security program.

Mark Wickersham (25:36):
Yeah, I think that's the thing with ai, that these firms should have some sort of policy in place because their employees are using it, whether it's they brought on an institutional capability or not, right? It's too productive of a tool for people not to be using or assuming that they're not using. So when it comes to weak links, Tony, what do you normally see as the weakest link? Does that kind of fall into a couple categories? What do you see there?

Tony Gebely (26:06):
Yeah, I would say the weakest link that we find almost every family we've worked with has a home that has infrastructure in it that was installed by an AV company several years ago and never updated, right? And these platforms, the ubiquity, Cisco, Fortinet, these hardware manufacturers that make routers, firewalls, et cetera, they put out patches that patch vulnerabilities every single month, and sometimes these patches will patch tens of vulnerabilities for a single device in a given month. So to hear from an AV vendor that a family worked with to install the network equipment two to three years ago that they've never updated the firmware, it just makes my head explode. I'm like, holy cow, this family might have a family office and they might have family office staff that are doing an okay job maintaining their cybersecurity posture for the family office, but they're unsafe in their own homes.

(27:04):
So typically, so I bring up AV companies because there are some AV companies that do a good job, but most of them are awful when it comes to cybersecurity. And most of them, when the family's building a home, they'll install home automation systems,

lighting systems, the AV equipment itself, but then also the networking equipment, and that's where that oversight starts. So what we'll typically do is if the family's working with an MSP or a managed service provider, IT firm for the family office, we'll bring them in to have oversight over all the networks and all their homes as well. So they keep everything up to date with the same processes they're using to keep the family offices infrastructure up to date. The other thing that we see that's still out there, just like it was several years ago, business email compromise, even with multifactor authentication in place, and this is just ridiculously prevalent.

(27:58):
It's scary, and this is an education piece. All of your staff need to be educated on how to spot social engineering attempts that could result in business email compromise. So let's just step back for a minute. Most firms don't have the systems or technology in place to even know if they've been a victim of a cyber attack. It shows up three months later where the bad actor has been in your email for three months and then they swap out an account number and use wire money away and it's gone. Then you find out, oh crap, my email is compromised months ago and we didn't know. So that's like the lowest level of cybersecurity maturity and not even have the systems in place to know that you've been impacted. So yes, we need some sort of technical controls around seeing who's accessing email and adding layers on top of multifactor authentication because it's really easy to get past MFA.

(28:52):
And just in 30 seconds, I'll explain to you how it happens. You receive an email, it takes you to what looks like the Microsoft login or the Google Workspace login. You didn't check the URL bar mistake number one, you type in your username and password, your phone shows your six digit code to log in. You thought you just logged in, so why wouldn't you enter the six digit code? You give it to the malicious actor on that screen, they go and enter it in within 30 seconds before it expires to the actual login, and now they're in as you, right? And now they're setting up systems like they're setting a mail forward to forward all your mail to them so they don't have to be logged in all the time, and whatever they can get access to from that point, they're going to start reading your email, learning your patterns.

(29:38):
So education's key here, that's one thing. But another thing is adding another layer on top of multifactor authentication. And the easiest way to do that if you're a Microsoft shop, is to talk to your IT staff or MSP about Microsoft Intune, which is a tool that will allow you to use your device as an additional signal on top of MFA and your username and password. So then you'll have username, password, MFA and my device. And then let's say you go out and buy a new laptop and you're a principal, or you buy an iPad and you want to access the files again, you have to enroll that new device into the system and it has to be involved. It's not difficult, but it's another layer. So you can't just be a bad actor and have username, password, social engineer, someone if you don't have the device you're not in. So we're working with families to implement Intune if they're a Microsoft shop, just to save themselves from that. So in short, I know that I've rambled a bit there, but in short, the two things we see the most are

business email compromise, still forever and insecure infrastructure primarily in the homes.

Mark Wickersham (30:48):
Carl, I also love the fact that we do the continuous kind of bite-sized training. Could you explain or talk about that a little bit more?

Carl Knecht (30:55):
Sure. We work with a firm that provides bite-size videos. They're produced, they're done really well. They're produced out out of Los Angeles, and it's great information. They're educational, they're informative, and it's quick. Sometimes sitting through hours long process of reviewing policies, procedures can get a little dry. So we try to kind of keep it interesting, keep it quick, keep it fun and down to earth. And I would also like to help people protect themselves at home. So these are things that they can share with their family. We provide number of services to help our employees protect their family as well, whether it's education or password protection. We know that information's going to go beyond our employees or the vulnerabilities go beyond our employees, it goes to their families, it goes to everyone else. So providing services for our staff as well as the families, try and push out that bubble to keep people secure even outside of our direct employees.

Mark Wickersham (32:09):
Tony, what would you say would be some best practices? Family offices should adopt

Tony Gebely (32:14):
Education. One to add on to what Carl just said and shop around for a good education program, so many of them are just boring, and what happens is a family office will put out all this training for their employees and extend it to the family members, and the family members are like, Nope, don't have time for this, and it sucks. So trying to find bite-sized pieces or even doing so, we do a lot of one-on-one training with family members. We don't find it useful to sit in a family meeting and talk to a grandfather in one corner that has an A OL address and doesn't even know how to log into it, and then his granddaughters in the other corner owns a law firm and has a cybersecurity team. The message isn't going to resonate with both of them. So we do a lot of that, but I mean, ultimately the message is to start with an assessment. Find a firm that can come in and provide you with a prioritized view of your risk. Even if you think you have your act together, you don't know where your weak links are, unless you've had a third party expert firm come in and try to find them for you. I mean, that is the starting point for any family.

Mark Wickersham (33:19):
Let's talk a little bit about ai. Obviously AI is evolving rapidly, one of the biggest trends in technology for sure. Certainly AI can be a source for good and a source for not so good. Tony, how are you seeing AI being deployed by the bad guys and how are you seeing AI being used as a protective measure?

Tony Gebely (33:43):
Yeah, so what you said is totally true. It's a double-edged sword here, right? We have it, so do the bad guys. So it's showing up on the bad guy side with you can go on a

chat GPT and have it write you malware. If you're that technical, you're also seeing Phish. You used to be able to spot phishing emails because they're all misspelled and they just looked and sounded ridiculous. It's not the case anymore. I mean, they're using chat GPT and other AI tools to write well-crafted emails to trick people. So they've got that on their side. On the good guy side, we're mostly seeing AI integrated into monitoring tools and other AI tools to look for malware like software, but also to reduce the number of alerts that some of these monitoring tools will spit out. So a monitoring tool that you'll have installed by an MSP on your endpoints will just look for anomalies, and when you first turn them on until you tune them and configure them, everything looks like an anomaly.

(34:52):
So there's like a learning period, and AI is really helpful in reducing the number of false positives that a monitoring tool will spit out. I mean, that's really deep and nerdy, but that's really where it's being used today. And then I mentioned using it to be able to write malware and other sorts of malicious code. This is important because a lot of old school antivirus and anti malware tools are looking for exact types of malware that it's seen before. It's called signature based. So looking for a signature, this is like, oh, that's that type of malware. But if I as a bad actor can take a known piece of malware, throw it into a GPT like tool and have it rewrite it, so now it's slightly unrecognizable from its current previous form. Now the signature-based antivirus tool can't find it. So these next generation antivirus tools use AI to look for malicious code that's not just based on its signature.

(35:51):
So that's how we're seeing it used on both sides. You're also seeing better phishing emails, but DeepFakes, et cetera, on the bad actor side, that's going to get worse and worse. I mean now they're little startups now they're like, oh, we can spot deep fix. We can spot ai, but pretty soon it's just not even going to be something that anybody can tell if it's AI or not. And there's going to be governments that are going to try to regulate it and slow it down, but unfortunately, the governments that aren't going to regulate it and slow it down probably where the bad actors are, and we're just going to be on the losing end of that, so it's going to get pretty weird.

Mark Wickersham (36:27):
Well, I mean, it used to be the gold standard on the wires was the callback. Right Now, the voice recognition, the callback seems to be AI doesn't need a whole lot of voice from a person to be able to completely replicate it, right?

Tony Gebely (36:41):
That's right. Yeah. And on that point though, there are two pieces of software that you should look into. If you wire a lot of money, conduit, security, and walrus, both of those platforms will verify each party before a wire is sent using their own proprietary verification methods. Walrus Fi will even guarantee the funds. If you send money, it doesn't reach point B, they'll guarantee it. So these two tools are kind of newish to the space, but they're providing people with peace of mind if you're wiring a lot of money. So definitely look into them if that's an issue or a concern of yours. What are you seeing,

Mark Wickersham (37:20):
Carl?

Carl Knecht (37:20):
I'm definitely seeing family offices, multifamily offices, engage ai. I think many of them are cautious from what I'm talking to them because of the security questions and concerns. So as you're reviewing AI and we're doing it for our company, what's the best way to and be proactive? What's the best way to implement ai? What are the vendors that we should be using and can use Microsoft? A lot of people are using the Microsoft 365 for email and Outlook and Word and everything else, and Microsoft has copilot, which is integrated in with the Microsoft stack and the Microsoft email platform. So I think utilizing well-known tools, going through a process of reviewing how AI is going to be used within the office, within the business, and then rolling it out in a way that is beneficial for the staffing employees, and there's clear guidelines on how to use it and when to use it. Definitely it's here. I don't think it's coming anymore. It's here. People are using it and be proactive in how you're going to utilize it.

Mark Wickersham (38:35):
Every family office at this point should have an AI policy. It's here. It's not something that they need to think about coming down the road. I'd like to end this on a bit of a personal note. Tony, I know that you're a tea enthusiast and just not a regular tea enthusiast. You actually have written books about it, but can you tell me a little bit about your love for tea and what makes the perfect cup of tea?

Tony Gebely (38:59):
Oh yeah, sure. Thanks for bringing that up. I've been studying tea for about 20 years now, written two books. My third one's coming out any day now, and it's always just been a passion of mine. I've traveled extensively throughout Asia studying tea processing. I spent a month in Vietnam working with their government earlier this year, helping them develop standards for a portion of their tea industry. So this thing, they call it a tea journey because once you get into tea, it just kind of drags you all over the world. And crazy thing, I even met my wife in tea. I mean everything. It is just kind of crazy. Anyway, so what makes a perfect cup of tea? Great question. I mean, I would say that using full loose leaves and steeping them at the right temperature and steeping them in a vessel where they can expand, not one of those cute little tea balls.

(39:56):
It's like this big because full leaves, once they're in the hot water will expand and you want the water to flow freely between them. Brewing high quality tea correctly will result in tea that has a depth of flavor that you likely haven't experienced before, and that would be naturally sweet. So you typically would not add milk, cream, sugar, anything to properly steeped high-end tea. And that's the world that I live in when I'm drinking tea. Something that a lot of people don't know is that tea comes from one plant. It's the cha sinensis plant, and from that plant you can create green, yellow, white oolong, black and fermented tea, and each of those six categories, there are thousands of teas produce worldwide, making tea the most diverse in flavor, more so than coffee and wine. When people hear that they're just really holy cow, then I'll typically do a tasting for someone and give them teas at opposite end of the

spectrum, just to show them that diversity of flavor. Some people come in and they're like, don't like tea. Like, whoa, wait a minute. There's like 20,000 types. Slow down, slow your roll. But anyway, that's my side on tea. Thanks for bringing that up.

Mark Wickersham (41:15):
Love a good cup of tea. I worked over in London for a few months and the afternoon tea became the part of the routine that I still enjoy today. So anyways, this has been great, gentlemen. I really appreciate both your time and being on the show and sharing. I think this is some really great information and I appreciate your insights.

Tony Gebely (41:36):
Thanks for the opportunity. Appreciate it.

Carl Knecht (41:38):
Thanks, Mark.