Speaker 1 (00:03):

Welcome to the Vandenack Weaver legal visionaries podcast brought to you by interactive legal here's your host Mary Vandenack

Speaker 2 (00:12):

Welcome to today's episode of Vandenack Weaver, legal visionaries, a weekly podcast discussing updated legal news, evolving methods of providing legal service and law practice issues. My name is Mary Vandenack founder and managing partner at Vandenack Weaver, LLC. I'll be your host. As we talk to experts from around the country about closely held business tax trusts and estates, legal technology, law firm, leadership and wellbeing. Before we start today's episode, I want to thank our sponsor. Here's the message from interactive legal.

Speaker 3 (00:51):

There's always a resistance to change, particularly with attorneys, attorneys like to look back at what's worked in the past, and that makes a lot of sense. But when you realize that with a good automated drafting system, you can do a better job for your clients. Deliver documents on a more timely fashion in a more consistent, in a more costly manner. If you're not a subscriber to interactive legal, I urge you to go to interactive legal.com and click on requested demo. And you'll be contacted about having a demonstration of interactive legal for you, which can be done right over the internet. Don't have to leave your office. No sales person will call. We can arrange it at a time and convenient for you. So please go to interactive legal.com and click on request and demo.

Speaker 2 (01:40):

These episode is on cybersecurity for lawyers. My guest is Ben Shore, senior content designer at Microsoft. We're going to talk about cybersecurity issues. Thanks for joining us. Ben

Speaker 4 (01:53):

Always enjoyed talking to you.

Speaker 2 (01:55):

Cyber security can seem really daunting to people who aren't in the field or even yeah. In the, well, I know it's daunting to me cause I'm not in the field and, and we've seen a lot of hacks and an increase. So how can we help them get started?

Speaker 4 (02:11):

The first thing that might help is to realize that perfect security isn't the goal. Okay. It's not even possible to be, to be perfect. You know, you don't, it's not that the goal isn't to make it impossible for somebody to break in the goal is to make them have to dangle Tom cruise from your ceiling to get in, right? You want to make it extremely difficult. That's what you want to do. And, and to do that really, it's a matter of getting the basics, right? If you just get the basics, right, you've gone a long way. I mean, obviously there's more you can do, but so many don't even get the basics, right? That's the first place to start. And the first one to understand there is that security is a process and not a product.

Speaker 2 (02:47):

So tell me a little bit more about what you mean when you say process, not a product.

Speaker 4 (02:52):

So a lot of people want to just write a check and having some box show up on their doorstep and they, they plug it in and it fixes everything. That's not how it works. You could buy every security product ever made in the history of computing and plug them all in, in your office. But if you don't deploy them correctly, if you don't manage them correctly, if you don't use them correctly, it's not going to work. It's not, you're not going to gain anything from that. So all the tech in the world is no good if you don't set it up. Right. And you've got to have those processes because security is fundamentally about people and not so much about technology. Obviously the technology helps. But one example would be the exit process. Okay. when people leave your firm, do you have a tried and true and thought out process, exit process for, for what happens?

Speaker 4 (03:36):

I had a lady come up to me at a conference. I was presenting at one time and she, I was, I was doing a session on outlook. I think it was, and she was waving her iPhone at me and she said, can you help me? I have my old firm's email accounts still in this someone outlook on my iPad or on my iPhone. How can I get rid of that? And I, you know, I looked to see what she's talking about. She had left that from six months ago and she still had the email, all the email from when she was working there on her iPhone, in her purse. And I'm thinking, oh my God, I mean, she was the administrator, she was the front administrator. She's got partner compensation spreadsheets. She's got all kinds of pretty sensitive stuff in her personal life that nobody bothered to ask about when she left.

Speaker 4 (04:16):

And this is even more true now because you know, we've just spent the last 18 months working from our dining room tables. You can almost guarantee that there are a lot of people out there in firms who have from data on their personal devices, in their houses. And if that person leaves your firm, do you have some process in place to make sure that that data gets deleted or reclaimed that's, that's an important, basic process that you need to have. The other thing I see a lot or have seen a lot is do you have a process for making sure to remove or disable them from your directory? I've been to firms where we look at their active directory, which is what is it, Microsoft 365, but whatever your particular directory services. And you'll see people listed in their directory that have worked at that firm in years, but they still have active accounts in the directory.

Speaker 4 (05:00):

And, and see, we ask, well, okay, who's this person. Oh, that was our, one of our paralegals. They left two years ago. Why are they still in your system? Why are they still have an active account that person could log in? So just a little basics like that, get that exit process. Right. the second thing to think about is shadow it that's, that's part, that's a process problem shadow. It is what happens when, when your users go around your policies and set up their own it solutions. So a good example of that would be, did people set their own remote access, right? Suddenly they have to work from their dining room table, but maybe they still need access to their computer at the office. Now, did you give them a way to do that? And if not, does that mean that they went out and set up their own remote access solution using some consumer level remote access solution that may not be secure?

Speaker 4 (05:45):

If so that means that maybe other people, other than people in your firm can now remotely access their desktop at the office. Did they set their own cloud file storage? Are they moving your from documents

on to Dropbox or, you know, Google without telling you maybe if you haven't given them a way to do it. And so it's really important to, to, to when you're approaching cyber security, that you're not the department of no, you're the department of how right when your users come to you and say, okay, I'm gonna need to work from home because of whatever reason for the next six months these are the access to these files that need access to these other resources. Don't just say no, because if you do that, they're going to figure out a way to do it themselves and you won't like it. Or, you know, the better way is how can we do that? Figure out how you can do it securely. That's the, that's really the way to do it. And then the third part, I would say here about the process is create a good security culture. That's so important.

Speaker 2 (06:39):

So what is a good security culture?

Speaker 4 (06:43):

So w a good security culture means that first of all, your people feel comfortable reporting a security issue to you, even if they made a mistake. So maybe they got caught by a phishing email and they accidentally clicked on the link and, ah, shoot, you know, they realize maybe too late that it was a phishing email. Okay. If they think they're gonna get punished, especially if they think they're going to get fired they may be reluctant to report that they maybe they may try to cover it up somehow or not be, not be forthcoming about it. So you want to make sure that, that you are open when they want to report a security issue, that you're not going to punish them if they made a mistake, okay. If they feel comfortable reporting that security issue, the second thing is be careful with security tests.

Speaker 4 (07:22):

Security tests are, are helpful, but you have to do them in the right way. There's been examples of firms that, you know, they send out an email that says, Hey everybody, you're getting a big bonus, click this link to learn about your tick, tick, to accept and receive your bonus. And they click the link. And what they get is that email or message that says this was a phishing test and you failed, huh? Shame on you. And that's, that's it, right? Well, now they're mad because one they're embarrassed. They feel the phishing test, but two, you just told them they were getting a bonus. They're not getting a bonus now they're kind of upset. So my suggestion is, if you insist on doing a phishing test that that promises bonuses or vacations or something, actually give them the bonus or the vacation, even if it's, even if you're going to, when they click the link, even if you're going to pop a message that says, okay, this was a phishing test.

Speaker 4 (08:05):

You are getting the bonus by the way. So don't worry, but you know, this one was a test and here's why my, my suggestion would be a different way to approach that would be to say, hi, everybody. We're going to, we're going to give you a bonus this month, just to, just to, you know, whatever it is, a hundred dollars, 200, whatever your bonus amount is. And all you have to do is read this next paragraph. And the next paragraph says, we will never ever make you click a link or open an attachment to accept a bonus or a vacation or some other reward. Please tell the person sitting next to you. And here's your bias. You get just show up in your paycheck. So, and do that every now and then, you know, say, Hey, by the way, we're gonna throw you a hundred bucks. Your kid's going to show up in your next paycheck and we will never make you click a link or open an attachment to get it. Just that might be a more effective, but you're drinking.

Speaker 2 (08:51):

So you mentioned basics. What are some of the basics? So I

Speaker 4 (08:55):

Tend to do, I think basics, I've been to a few kind of broad categories. The, the first one being authentication, which is a fancy word for proving who you are, that you are, who you say you are second category be devices. So protecting your computers, your mobile devices and so forth. And that did get a lot harder in the COVID era. You know, when people were scattered to the wind your security perimeter, you know, now includes everybody's dining room table which is, which is very difficult to manage. And then finally awareness would be the third category that I, I like to talk about, which is you know, security, as I said is fundamentally about people. And you want everything. You want to do everything you can do to help people make good cybersecurity decisions. Because at the end of the day, you're not going to be standing behind them. When that phishing email comes in, right? You're not going to be standing behind them when they find a USB drive on the ground, outside your office and decide to pick it up and do something with it, right? So they need to make that decision themselves in those moments. And you want them to make good decisions.

Speaker 2 (09:49):

We are going to take a brief break from our episode for a word from one of our sponsors, Carson private client,

Speaker 5 (09:57):

The planning focuses on liquidity management and charges you a fee based on a percentage of your assets, but entrepreneurs typically invest in their business resulting in light liquidity. That requires a unique strategy at Carson private client. We provide a proactive and holistic strategy for building and protecting your wealth. Our mission is to alleviate the stresses and the burdens of coordinating all of those financial strategies. Carson, private client will work with your current team of advisors to customize a strategy that manages all aspects of your life and wealth, giving you back the time to focus on what matters most complex needs require sophisticated solutions. Reach out to our office at 4 0 2 7 7 9 8 9 8 9. To schedule your consultation. Investment advisory services offered through CWM LLC, an sec, registered investment advisor. Okay.

Speaker 2 (10:57):

We continue our episode. Okay. Let's talk about authentication.

Speaker 4 (11:02):

So, the authentication is so fundamental to security. It's, it's how you control access to your accounts and your data. And so there's three things I want to highlight with authentication. The first one is strong and unique passwords. You've heard us say this forever. Okay. but let me tell you why strong passwords matter. Cause we get a lot of people are like, oh, okay. Yeah, I've got a really great password. You know, it's, it's my college mascot and my year of birth and, you know, Fred Flintstones, middle name and you know, my favorite band all truncated together. Okay, cool. It's 41 characters long. That's great. But they use it everywhere. And the problem with that is let's say that your favorite toy shop he'll when toys gets hacked, right? Their website gets hacked because their security is not super good. And your username and password, your username is probably your email address.

Speaker 4 (11:50):

Cause that usually is these days and your password is your super mega good 41 character password. Well, once that gets out what happens is the crooks take that username and password and they try it everywhere. They try it at the banking at the banks, they try it at the shopping sites. They tried it. If your domain name is your, if your email address is your work email address, they'll try it at your work site because they know what company you work for because of your, your domain name. So that's got a credential stuffing attack. It's one of the most common attacks we see these days. And so when you reuse that password, even if it's a great password, all it takes is for one kind of second tier vendor to get hacked and lose their username and password data. And suddenly you're using and password is everywhere and that's bad.

Speaker 4 (12:34):

So that's why we definitely encourage using a password manager Microsoft edge, for example, there's, there's plenty of them. Last pass is one. I can't think of all the rest of them right now, but there's a number of them out there. If you pick up a reputable password manager, that's great. Microsoft edge has password management built into it. A lot of the browsers do now too. Edge has a password generator in it now, so that when you go to create an account somewhere or to change your password somewhere, when you click on that password field edge can, if you want it to edge, can suggest a strong password for you, which is totally random. It's just as long, it's a 14 character string of random letters and numbers, and then edge will remember it for you. So when you come back to that site edge can fill it in for you.

Speaker 4 (13:14):

So strong and unique passwords, don't use the same password everywhere and make sure it's a strong password. Second thing, I probably shouldn't say this, the first thing, cause honestly, it's the number one. Most important thing you can do for cybersecurity is turn on multifactor authentication, which is also sometimes called a two-step verification. And basically what that does is when you go to sign in somewhere, you, you put in your username and password, and then it will ask you for a second kind of authentication. Usually that's in the form of what we call a one-time passcode. Most people see, I've seen that where like sends you a text message with a string of numbers in it, right? That's okay. The

PA the text message method is not the most secure, but it's better than nothing. Using an authenticator app on your smartphone is a better way to do it.

Speaker 4 (13:59):

Microsoft, we have a free Microsoft authenticator app that works everywhere, Amazon and, and Twitter. And you name it it’s works everywhere, but there are other authentic erupts as well. You don't have to use ours. The authentic reps are more secure because that all happens locally. The codes are generated locally and they change every 30 seconds, which is awesome. So what that means is that when somebody let's say somebody has stolen your password, right? Maybe tailwind toys got hacked, right? Your username and passwords out there, they go to your bank and go to bank of America, and they try to sign in with your username and password, and maybe they got lucky and you did reuse your password. So they now have signed into a tribe to sign to bank of America with your username and password. Well, if you've got the two factor authentication turned on, it'll prompt them then for the second factor where they might have your username and password, but they almost certainly don't have your smartphone.

Speaker 4 (14:44):

So now they're stuck. They can't get in. And with Microsoft 365, same thing, almost every online as you to turn on multifactor authentication and it blocks 99% of the credential attacks we see it's, it's really that important, and it's not really the hassle you think it is. I almost never get prompted for my second factor, because if you're signing in on the same device, you always sign in on the site, recognizes that, and doesn't prompt you every time for your second factor. So, for example, when I sign in at work here, I'm signing it at my office desktop. I need my username and password, but I don't need my second factor because this is my usual device. Now, if I sign in on a device I've never signed into before, or if I've changed my password, then it'll prompt me for the second factor.

Speaker 4 (15:25):

And then the last thing I wanted to mention is a concept called least privilege and least privilege is sort of keeping people in their swim lanes, right? Give them only access to what they need when they need it. I was at a firm once where their receptionist had access to all their HR data. And the reason is because at one time, three years ago, when they put in their new HR system, the receptionist got tasked with entering people's, like birthdays and, and home addresses and doing data entry. And they, and it was simpler for them to just give the, that HR person that receptionist all access. Well, they never took it away. First of all, I shouldn't give them all access anyway, but they never took it away, which means that person, that receptionist, but now look up payroll all kinds of other, and anything in the HR system.

Speaker 4 (16:06):

They could go in and look at it if they want it to. We also see this a lot with firms where if you have people that practice in one practice area, and they only do that, you know, I haven't been at firms where they have immigration attorneys and that that attorney only practices immigration, but the firm has other practice hurts. Well, does that immigration attorney need to have access to the documents in the wills and estates practice area? Do they need access to contract law? Do they need access to all these other practice areas you may have? Probably not. And one of the best ways to minimize the damage from an attack from a successful attack like ransomware is if you keep people in that least privilege where they only have access to the files they need, when they need it, then the malware, any malware, they might get your immigration files in this hypothetical, but not everything. So keep people in those swim lanes with least privilege. That's, that's the third part of, of authentication.

Speaker 3 (16:55):

So what about devices then?

Speaker 4 (16:57):

Devices is a little simpler. Devices is just about protecting those, those computers, those mobile devices. It's largely, it's about staying up to date. That's the most important thing keeping your operating system update, whether it's windows or Mac or mobile, right? When those updates come in, please install them. I, it's so frustrating to me when I see these news reports, you know, I get all the trade press and all the, the back channels about attacks out in the world because cybersecurity is what I do. And so often I'll see, you know, this company got breached and the attackers used a vulnerability that had been patched in January. And you're just like, you know, five months later, they hadn't installed that patch yet. And if they had just installed the patch, right, this attack wouldn't have happened. It couldn't be, it couldn't have been, wouldn't have been successful.

Speaker 4 (17:40):

And so just install the patches that that's a first step. Okay. But it's not just the operating system. It's also your apps and your browsers. So Microsoft, whether it's Microsoft office or some other third party app that you're using your web browsers, whether it's ads or Chrome or Firefox, opera, whatever browser you're using it, those updates come up pretty regularly. The browser is probably the most important app to pass these days because the browser is such a big you use it a lot. Everybody uses their browser almost every day, probably all day. And it's an avenue that a lot of the attackers will go after because it's so widespread. And so definitely get those updates installed on your browser when they come out and well, I've heard people say, well, I've got 27 tabs open, and I don't want to do the restart on my browser to apply the updates.

Speaker 4 (18:21):

Cause I'll, I'll have to reopen all my tabs, all the modern browsers, definitely edge and Chrome. I'm sure Firefox does too. All the modern browsers. Now, when you do that, restart to apply updates, we'll reopen your tabs for you when that browser reopens. So you're not going to lose your tabs get those, get those apps and stuff. And then the last part I want to say about staying up to date is don't overlook your devices, printers, firewalls, wireless routers, you know, all those hardware devices. And of course the, the, the computers and the mobile devices too they'll have firmware on them. That firmware gets updated from time to time. And those updates can be critical for your security as well. So have a process in place. We talked, remember we talked at the beginning about security as a process, not a product.

Speaker 4 (19:02):

Okay. I have a process in place that you regularly check where your, it, people rarely check your firewalls, your riders, your network, gear your printers, and make sure that they have the latest firmware installed. That can be a big improvement to your security. And it's super easy to do. Second one would be secure your Wi-Fi. A lot of people get lazy. They they've either used a lame password on their Wi-Fi or no password at all. Have a password on your Wi-Fi and you need that. That should be WPA two or better. WPA three is now getting pretty widespread acceptance. If your Wi-Fi is using either just WPA version one, WPA, or w E P, you need to upgrade that now, because those are very insecure. So you need WPA or two or better with a good password.

Speaker 4 (19:49):

I would recommend now, you know, when we've got so many people working remotely, even if they're only working remotely, part-time, I would offer to have your it people to pay, to have your it, people check their home Wi-Fi, you know, just tell you, I mean, you probably can't sit on it and would be a little rude anyway, probably, but maybe you can. It's just not, it would still be a little rude, but I would suggest say, Hey, if you'd like, I will pay our team, our it people to spend an hour with you at your house and just make sure your Wi-Fi is secure. Okay. Easy thing to do. And it can make a big difference because if somebody is using insecure Wi-Fi at their home to access your firm's resources, that could be a potential vulnerability. And the third thing I'd say about secure Wi-Fi is don't remember public networks.

Speaker 4 (20:27):

People go into their favorite coffee shop and they sign into the Wi-Fi and they set their laptop or their mobile phone to remember that network so that it always just automatically connects to it. Yeah, don't do that. There is a whole class of attacks out there called evil twin attacks where somebody sets up a fake Wi-Fi access point. I think John summit has actually demonstrated this at tech show a few times or

Lincoln made, maybe it has where you can set up a fake Wi-Fi access point with that commonly known, you know, Starbucks Hilton, O'Hare free Wi-Fi, whatever SSI D and you can trick people's devices into connecting to them without the person even knowing it. And then you can do all kinds of bad things. So don't remember public failure, never, never set your device to remember it. I would never, you don't control.

Speaker 4 (21:10):

That's the third part of streaming Wi-Fi I guess the last part would just be physical security. I see a lot of people who don't lock their screen like their mobile device doesn't require a password or a fingerprint or face ID to unlock. You definitely need to have that. Because otherwise, if somebody finds your device, they can do anything they want with it. If they find it and it's unlocked. So, your devices should always be secured with something face ID, fingerprint, pin and St for your windows and Mac devices as well. If they go to sleep or their screensaver kicks in, there should be a, we should have to sign into Amman.

Speaker 2 (21:44):

So what about awareness?

Speaker 4 (21:45):

So awareness is about just staying informed. You don't have to be an expert. You don't have to spend all day reading the trade press. You know, you don't have to get the level of, of, of Intel that I get on this stuff. This is what I do for a living. It's not, probably not what you do for a living. So, but there's a few things you can do just to, just to be aware of some of the top trends and most common threats. And if you don't have the time or the interest in doing that, that's okay. Not everybody does consider hiring the smartest kid in class to do it for you. You know, there's a lot of, of good it folks out there. It partners who can be your trusted advisor, you know you guys are all lawyers, you probably don't expect your clients to be experts in tax law and immigration law and whatever other, but over here, you all you practice, right.

Speaker 4 (22:25):

They hired you to be that expert. So don't be afraid to hire somebody to be your expert on cybersecurity. There's a lot of great firms out there that can do it. And the second thing I'd say is talk to your staff about it on a regular basis. You don't have to make it a, you know, and now we're going to spend the next two hours talking about cybersecurity. This week you know, you can be brief, it can be a tidbit. If you do a newsletter, it can be a, the more, you know, the little thing at the end, it can be you know, cyber security minute in your, in your weekly staff meeting, right? It doesn't have to be these long diatribes or these long half day trainings. People, our research has actually shown that people really like it when they learn things in those little bite-sized tidbits. And so don't be shy to share it as tips. And it, it can be more valuable to share a tip a week over the long-term months than to try to cram two hours into them once a year. That's not always that good. So consider, you know, definitely keep, keep the communication flowing though.

Speaker 2 (23:22):

So is there anything that Microsoft 365 is offering to help?

Speaker 4 (23:26):

There is, we've got a lot of security features in Microsoft, 365, probably the most important one is a feature called security defaults. You know, this is radio, not video, so I can't show it to you, but if you, if you sign into your admin console in Microsoft 365 and go into Azure active directory, you'll find it back there. You can go, you can Google or internet search for, for Microsoft 365 security defaults. And you'll find a great article that shows you exactly how to do it really easy. Once you get back there, it's just a check box. Now, if you have a brand new Microsoft, 365 subscription or a fairly new one, it's probably already on, but if you have an older one, it might not be a, and so just go in and confirm that it's fine, and it's literally a checkbox. And when you click it, then Microsoft 365 is going to turn on a number of features for you that are critical to cyber security.

Speaker 4 (24:10):

One of them being multifactor authentication and multifactor authentication for all of your user accounts. So, security defaults that that's a first thing to do, and it's easy. The second thing would be safe, links safe, like a, like a safe, a bank vault, safe and links like hyperlinks, like web links, safe links. You can, again, internet search for that. If you turn that on in Microsoft 365, that's a service that we do where anytime somebody gets a hyperlink in an email, or now we've extended it to Microsoft teams what'll happen is when they click on it. And 365, we'll check it first to see if it's a known phishing attack, a known malware site. You know, obviously we want you to be smart about what you click on to it, click on unattached, unexpected links anyway, but if you click on a link, you know this is just another layer of protection to reduce your risk.

Speaker 4 (25:00):

We also have a bunch of other settings in there. There's a whole thing in exchange online for anti-phishing that can help identify spoofed emails and incoming emails. It's spoofed. You can set up your outbound message at your, at your, your exchange server so that it uses the authentication mechanisms going outbound, so that it's harder for people to spoof your messages to other people. But yeah, there's a ton of things in Microsoft, 365, and it can get a little confusing, but this is another place where you might want to hire a partner to help you. So, any other tips? Yeah. have good tested backups. That's the tested part is that when people miss a lot of people do backups, but they don't test their backups. When I was in private practice, I got called into a firm cause they'd had a server crash and they'd been doing backups.

Speaker 4 (25:43):

They'd had, this was back when they were using tapes for backups. And they had tape backups. They'd been doing them every night. And so we came in to help them get their new server all set up and restore from their backups. And we discovered that the backup state been doing every night, hadn't actually worked in over a year, but they didn't know it. Wow. Yeah. So they had no backups as well. They had backups, their backups were over a year old. That was a very bad situation for that firm. So that's the first test, your backups and the easy way. When, when do you see when to test your backers? Most backup systems provide a good testing system, but if you want to, here's another way you can test your backups, create a test file. It can just be a word document called test.

Speaker 4 (26:18):

Doesn't even have anything in it. Store that alongside your real documents, just keep I call it test. Right. And then what you do is let it get backed up along with all your other files. And then once every quarter, twice a year, whatever, go in and delete that test file. And then see if you can recover it. If you can't

recover that test file from your backups, then either your backups aren't working or you don't know how to restore files either way. That's a problem you want to solve before you need to solve. And so that's an easy way to task. There are more robust ways to test, but that's a simple thing that everybody could do. Second is have a business continuity and disaster recovery plan. You know, we shouldn't have to tell lawyers to plan, right? We were supposed to all be all about, about making sensible plans but a business continuity and disaster recovery plan.

Speaker 4 (27:02):

That's, it's as simple as identifying what resources are key to your firm, to the operation of your firm, people, equipment, places outside vendors, information, all sorts of things, whatever it's critical to the, to the operation of your firm and think about what you'd do. If you lost access to those things, right. You wake up tomorrow and that person is, is seriously ill and unavailable or that building burned down or that computer crashed. Right? What do you, how do you, how do you keep the firm running? If that happens? What's our backup plan? What are we going to do? Right. We also used to say alternate location. Like, what do you do? Why kind of did there with them if your building burned down. But you know, now that's kind of solved itself because we've all been working from our dining rooms, but you know, have a plan for that.

Speaker 4 (27:45):

You, you want to learn to swim while the sun is shining. Not all the floods are coming. Right. so, so make sure you've got a plan for what to do in those situations. And sometimes people ask me, what's the difference? You know, business continuity plan and disaster recovery plan, right? Disaster recovery is what happens when your business continuity plan fails. So that's, that's what you've got to have that plan. And then the last thing I'd recommend is, you know, get a security assessment done. There are so many good firms out there that can do it and it doesn't have to be expensive. People are worried that, oh, it's gonna cost me tens of thousands of dollars, not necessarily it can be very reasonably priced and you can get them to give you a pretty good report on what your current security posture is for people who do this all day for a living and can tell you what you need to fix. And you might be pleasantly surprised to discover it's not as expensive or challenging as you think to fix those problems. It's not expensive to fix them ahead of time. It can be very expensive to fix them after the fact.

Speaker 2 (28:36):

So it seems like there's new scams and security issues that come up every day. And one of my solutions has been just following you on social media. And I have other people in my office and our it people follow you. But is there anything else that we can do just to keep up?

Speaker 4 (28:51):

Yeah. Social media can definitely help. I thank you very much for following me. I'm happy to, I'm happy that people want to do that. I do try to share it for you. So please feel info. There's a lot of other good people on social media to follow also. And also since they're podcast listeners, since they're hearing this I'm gonna see just two podcasts that they might like first one's from it, world Canada, it's called cybersecurity today. It's a daily podcast. It's about five minutes long and it's very accessible and he just gives you a quick briefing of stuff that people are. They're seeing out in the wild of cyber-attacks and just things happening. And pretty much anybody could understand that he's not overly technical, which is great. And just a great little briefing on here's what's happening today. Cybersecurity today from it broke Canada. The second one is a weekly podcast from the cyber wire group called hacking humans. It's

about a 30 minute podcast comes out once a week, and it's a really interesting exploration of different scams that they're seeing phishing attacks and other kinds of cyber security stuff like that. Really very entertaining. Again, it's, it's something that you don't have to be a cyber security expert to understand. So yeah, hacking humans by the, from the cyber wire group. That's another podcast I really recommend.

Speaker 2 (29:55):

Well, Ben, thanks for being with us today. As we get to the end of our episode, I want to thank our sponsors, interactive, legal, and Carson, private client. That's all for now. Thanks for listening to this week's episode and stay tuned for our weekly releases

Speaker 6 (30:15):

Hurrdat media production.