Narrator: Welcome to "Beyond Bitewings, "The Business Side of Dentistry," brought to you by Edwards & Associates, PC. Join us as we discuss how to build your dental practice, optimize your income, and plan for your future. This podcast is distributed with the understanding that Edwards & Associates, PC is not rendering legal, accounting, or professional advice. Listeners should consult with their business advisors before acting on any of the information that is shared. At Edwards & Associates, PC, our business is the business of dentistry. For help or more information, visit our website at eandassociates.com.

Ash: Hello and welcome to another episode of "Beyond Bitewings." In today's episode, we will be talking about the importance of paying attention to your practice's cybersecurity. And to expand more on the subject matter, we have a special guest here, Ieshea Hollins, who owns a company called Direnzic Technology. She's originally based from Louisiana and has been in this industry for over 10 years. However, she has recently opened up a second location right here in the DFW Metroplex. And again, our regular, Robert, is also here.

Robert: I'm here.

Ash: Hi. So, you know, without further ado, tell us a little bit about yourself, Ieshea.

Robert: Let me interrupt right now. How'd you come up with the name of your company? That's so unusual.

Ieshea: Thanks for asking, and thanks for having me on. It's actually digital forensics. So I actually put the two words together. It's actually what we originally started out doing, which was digital forensics, working with law enforcement and attorneys with regards to getting prepared to go to court.

Robert: Very interesting.

Ieshea: Yeah.

Robert: Very interesting. Great.

Ash: What is cybersecurity? I mean, I know a lot of us have somewhat of an idea of what it is but, you know, you're the expert. If you had to define it, how would you define it?

Ieshea: I love that question. I feel like, especially in today's time, a lot of us, we throw the word cybersecurity around, right? Oh, that's cybersecurity. And really, what it is, it's about knowing or protecting your data, right? From bad players, okay? So it's digital data content that most organizations or individuals have where basically it's stored somewhere and it needs to be protected and, or watched, monitored. And so that's basically the crux of cybersecurity.

Ash: I see. So for let's say a dentist who retains confidential information of their patients, this would be an important subject matter to pay attention to.

Robert: And it's totally underutilized. I mean, I can't imagine how many of our clients just ignore it completely.

Ieshea: Oh, exactly.

Robert: I think I read somewhere that the wrong approach to cybersecurity is to stick your head in the sand, and I think that's what 90% of our clients do.

Ieshea: Yes.

Robert: I don't think they've taken any steps to protect their data. So knowing that we work with a lot of dentists, what would be your advice? I mean, give 'em some actionable items that they can call you and have help you implement.

Ieshea: Certainly. Yes, I think with a lot of people too, though, it's we do nothing because we really, a couple of things, we assume that it's gonna be outside of our budget, right? I didn't think about that, and I really don't wanna add it to my budget. Or it's something that I don't understand enough of. And so because I don't understand it, I really don't wanna sit at this table, right? And start having this back-and-forth. And we all get those sales calls, right? You need blah, blah, blah. It's gonna cost you blah, blah, blah, right? And who wants that, right? And so when you don't have IT person with that particular skillset on your team, you tend to avoid that, which leaves you completely at risk. So what we do is we definitely, we talk to some of our smaller entities and let them know, sometimes just reach out and do a consultation, right? Just have someone come out and take a look at what do your systems look like? We heavily encourage our clients to get a vulnerability assessment. So what's a vulnerability assessment? It's an assessment where we come in and we're gonna take a look at what are your systems? How are they set up? And where are you weak, right? And so we can give you back a report that says, hey, you have this or this, that these ports should be closed and you have 'em open. And maybe in some cases, you've actually had an employee that you retired or fired, right? And they still have complete access to the systems. And nobody, again, because our IT department, most of our IT department, they're great. No harm to the IT, but their jobs was to keep the lights on, make sure that the internet's working, make sure that the PCs come up, that we can print, right? So when we start looking beyond the infrastructure, right? So that's why you want somebody else to come in and say, hey, no harm, no foul to IT, but go just a little bit beyond. And when we go a little bit beyond, what we show you is exactly how you look to somebody that may want to do you harm, right? We do that in the beginning.

Robert: Hmm, interesting. 'Cause most of our clients don't have IT people. They have to contract that out.

Ieshea: Exactly.

Robert: And they're more worried about operations rather than protection from something that probably is never gonna happen to me.

Ieshea: Oh, my God. You would be amazed at how often I hear that. Either it'll never happen to me because it's never happened to me or, you know, well, even if it does, they're not really gonna, it's not really gonna be a big impact. Well, first of all, more often than not, once we start taking a look behind the curtains, right? We can peek behind the curtains, more often than not, and this is not anything for anybody to be ashamed of, most businesses have already endured a breach. They just didn't know, right? Because they didn't go looking for it.

Robert: So you can tell?

Ieshea: Yes, we can tell.

Robert: Wow. That's, you know, I would ask how, but that might take more than the time we have to explain.

Ieshea: Give me a call, we can do a consultation.

Robert: Now, see, I learned something new. I didn't know that you could tell if a system had been breached.

Ieshea: Uh-hmm, yes. So again, let's think about your networks or even with your router. A lot of people don't look at the traffic, right? So, and again, let's go back to sometimes we'll talk about things that we'll implement and put in. So you buy a system and you put it in, but as you just said, most of your IT is outsourced. So who's looking at the logs? If there's unusual traffic in or out of your network, who's reviewing those logs? And if there's unusual activity, and then even if you were to notice, what's your next steps? Who do you call? So it goes back to, for us, that's another service that we provide, those cybersecurity strategic plans. We start having those conversations. When do you bubble this up? Who do you call? Do you call the head dentist, right? Is that actually his area of expertise? Or who do you want me to reach out to? You want me to call your IT company, you know? And how many dentists does he have? We have to keep in mind when you start talking about a framework, when you start talking about outsourcing certain things, so how many other dentists is he working with? And so maybe the breach didn't happen to you. Maybe the breach happened to your outsourced IT. And again, let's not, I don't wanna get pelted by a bunch of IT companies, right? I love my IT. I am IT, right? But you have to think about, think about, let's go back to Target. Target was not breached because Target was breached.

Robert: It was a vendor, wasn't it?

Ieshea: It was a vendor, HVAC. So the air conditioner company, the HVAC company, which is a smaller company. And that's why it's so critical that we start paying attention to what we do for small businesses. That's why one of our areas, small to mid-sized businesses. Our larger ones, they're gonna have some of the cybersecurity framework and things that are done.

Robert: Well, they have IT on staff.

Ieshea: That's right.

Robert: Yeah.

Ieshea: Yeah. They have more-

Robert: Of a defense.

Ieshea: Exactly. Exactly. And for, you know, our smaller ones, hey, everything worked today. We were great, right? And so when you say let's double-back and let's take a look, well, maybe somewhere along the line, something got breached that was a kink in your armor, and nobody stopped to say, "Hey, what happened here?" And we can stop and say, "Hey, what happened right here?" Right? And so the what happened here, usually, we're gonna find that there may or may not have been a breach. But also, it's all, you know, we're gonna find something that happened right there. And then, right here, right? So somewhere along the way and we can then start, you know, creating, you know, what that looked like.

Robert: So if you have a good firewall and antivirus software, is that enough to protect you?

Ieshea: That's a great step in the right direction. But it's not enough.

Robert: Okay, okay. Well, of course, you know, what everybody's gonna ask and you alluded to it when you first started talking, it's like cost. So describe to us how a budget for something like this, if you got a dental office and you've got, I don't know, five or six employees, maybe seven or eight, what kind of budget can you expect to spend just for the vulnerability assessment?

Ieshea: So your vulnerability assessments, again, depending on the size, so I don't wanna, you know, get pigeonholed into pricing, but you can look anywhere around the eight to $15,000 mark. But again, you wanna look there with regards to what does this look like? It'll give you the baseline you need for the year, right? So we're not saying that you need to, you know, that this might be something that you actually have to start, oh my goodness, and then, you know, it may be too much. But you can't afford to not have it, right? A lot of people, you get caught up in the what it cost me today. And then, you fail to realize you can lose your entire practice because you didn't have the 8,000 to the 15,000. Sometimes, these are just things you need to put in your budget, right? Ongoing IT support. I mean, what are you paying for that every month, right? So when you're saying eight to $15,000 potentially to get your report back, then, you know, you're looking at even if you broke that up, that's a little bit more than, what, $1000 a month? Just to get back what your framework, how you look. It just varies. It depends on the site, though.

Robert: Okay, so what is it that you can do to prevent people's systems from being breached?

Ieshea: Well, again, so that's a couple of things, right? So we talked about the vulnerability assessment. You can go a little bit further than the vulnerability assessment, and you can talk about penetration testing. Penetration testing says, we take a look, we see your vulnerabilities, we actually breached with your permission. We actually do a targeted attack to your systems.

Robert: Oh wow.

Ieshea: And we can come back and show you, see, if I had not been working for you, this is what I would have had access to. And we can show you access to your financial service. We can show you access to your HR. We can show you access to your medical records. Literally. It depends on where your servers reside, what information is there, we can actually give that back to you. The cybersecurity strategic planning, it's what do you have? Sometimes, a lot of virus systems, they're just too old. Like, you'll be amazed how many times we go in and, well, my computer still works and the Windows 7 still works, right? But it's not been supported in, you know, how long. Who patched it? So when you start talking about those types of things, then that's what we are able to come in and do. And we also provide training as well. Having those conversations with your staff to say, hey, you know, these are some of the things we don't wanna do, we do wanna do. One of the services that we offer, I absolutely love it. You know, sometimes, the client loves it. They love it after, right? But we take those policies and procedures and we say, "Okay, so this is what you think your people are gonna do "if there was an incident? "Yeah, yeah. We're good." Okay. And then, we basically kinda throw a bomb in there, right? It's like, "Okay, here, there's a sample of a ransomware attack," or there's a sample of, you know, an infestation within your network. And we show you just how long it takes for your employees to actually follow what you thought was in those policies and procedures. How long did it take him to call? How long would you guys have been shut down? Various things like, and we'll take a look at that. And then, because it's us, then we say, "Okay, it's been a couple hours. "You've seen enough." We shut it down, put everything back online, and then we go off-site and we say, "Now, let's review." We're here. What are our lessons learned? What do we learn from here? And those are the things that we will tell our clients that need to be done, some steps.

Ash: Okay. That's amazing. It's like a drill, a fire drill.

Ieshea: It is. Disaster recovery planning.

Robert: That's pretty much what it is, a fire drill.

Ash: Oh, my goodness. That's crazy. I bet if the employees are not aware of it, that could really freak them out.

Ieshea: They're not aware. The only ones aware are the owners.

Ash: I see.

Ieshea: Or the executive team, uh-hmm.

Ash: That's great. Amazing. So it's not just the patient records from what I'm hearing. They could lose a lot more. You're saying access to their financial accounts.

Ieshea: Yes.

Ash: I mean, you know, we know a lot of-

Robert: Well, the big exposure, I think for the the dental offices, maybe I'm wrong, but I'd think the big exposure is the nature of the patient records because it's got their addresses, it's got their credit card information, it's got their social security numbers. That's all in there, and that stuff is worth how much on the dark web?

Ieshea: It's worth a lot. I mean, oftentimes, we talk about identity theft as if the only reason why a person steals your identity is to get to your bank account, right? And depends on what's in your bank account, you don't really care. "Oh, there's not much in there. They can have it." Right? But excuse me, from the dentist's perspective, according to HIPAA, there is, you know, the breach to your reputation, number one. And then, the number of attacks that you have, you actually have to report. And then, in some cases, you can be fined by the day or by the week for how long it takes you to get, because you were outta compliance, you fell outside of compliance, so you actually have to get back within compliance. And you can be fined by the day until, per record, until you're back in line.

Robert: Okay.

Ieshea: From your patient's perspective, you've just left them wide open, right? And so that breach to their security can go a lot farther. Think about, you have copies of what they're allergic to. You have copies of just various things that have gone on in their lives. So what happens if their medical records are breached for ill gain for different reasons, right? So we have to look beyond just "they could steal my bank account "and my bank account would cover that." We actually-

Robert: Well, and I know it's not just stealing the bank account because if they had that information, not only could they empty your bank account, but they can open credit in your name and actually, you know, buy things. And, you know, you get the bills in the mail.

Ieshea: That's right.

Robert: Yeah.

Ieshea: We've had entire cases where not only is your identity stolen, again, think beyond just a bank account. If I can now say that I am you, and I'm now declaring myself as the DDS, right? But I'm no longer in Dallas, Texas, but I am you, and I'm now in Alta, Utah, right? And I'm claiming that I'm a dentist because I've mirrored your identity. So I've actually got an entire practice, and I'm doing an entire, who's checking those things? You see what I'm saying?

Robert: Yeah.

Ieshea: There are cases where we've had to go and literally had to go back and forth to prove when this other facility was opened. And how long was it established? What has been done? So when you start getting into the digital forensics and stuff, like it goes beyond. You actually

have to know, when was the last time you did a background check on yourself and seen some of the things that are out there? So oftentimes, we don't talk beyond, oh, well, you know, my identity was stolen and they got into my bank account. No, they also show that I live somewhere I don't. And then, who's cleaning that up?

Robert: Yeah, I've never thought about running a background check on myself.

Ieshea: Most people don't.

Robert: Yeah, I mean, I know I'm a great guy, so what else is there?

Ieshea: There you go. Yes, you are.

Robert: Now, I understand. So how much exposure do you think some of our clients' dental offices would have to various different attacks, you know, phishing attacks or vishing or smishing or any of those?

Ieshea: Dental offices and most, and I'll go back to most small businesses, they are one of the most attacked entities because they're the least protected, hands down. So to answer your question, a lot of them. A lot of them are at risk because a lot of them, they really don't know where to turn. In some cases, they just really don't know who to reach out to. More often than not, the answer is I have virus, you know, software on my system, and I may or may not have a VPN, right? And so they feel like, "I've done my due diligence, I should be good." But really and truthfully, we are, yeah, we are long past the days where that is enough.

Robert: Okay, okay. I know in our business, every single day, I get phishing emails trying to get me to click on something that I know I shouldn't click on.

Ieshea: Mm-hmm.

Robert: But you know, I worry about my 24 other employees clicking on that. And sometimes, I'll get an email from one of the employees that says, "Hey, did you send me an email?" Because it didn't come from me, you know, but it has my name on it.

Ieshea: That's right.

Robert: So I think all, I don't know about all small businesses, but I know we get those daily, multiple times a day.

Ieshea: Mm-hmm.

Robert: And you just gotta kinda use your common sense to know if it's real or not or if it makes sense.

Ieshea: Yeah. So I like to tell people to also just be diligent. We are in a time where more often than not, it's better that you double-check, right? You get an email and it's asking something

outside of the norm. Anything with links inside of the email, let's avoid those, right? Or definitely double-check. "Hey, did you send me something with a link in it "before I click it?" Right? And a lot of people, oh, that's just overkill, no, it's really not. It's-

Robert: See, sometimes I think I'm being paranoid. I got one this morning. I forwarded it to my assistant. I said, "I don't recognize this name." She emailed me back and said, "Well, that's so and so, the previous CPA. "He's sending you their records." I thought, "Oh, well I'm embarrassed."

Ieshea: No, 'cause you may have saved a lot of time and energy and effort just by doing just that. But you see how easy what you just did implementing that step? Regardless of the embarrassment that you may have felt after you verified, but sometimes it's just that easy. One click could have actually destroyed a lot of stuff-

Robert: Oh yeah.

Ieshea: versus one phone call or one forward to your assistant, and she's able to say, "No, this is who this is," right? And so now we can say, "Okay, we can safely click this."

Robert: And I know throughout my life, I've kinda learned to view everything as a game. And so I literally get these emails every day.

Ieshea: Yes.

Robert: Multiple times.

Ieshea: Yes.

Robert: And so it's sort of, to me, it's a game to pick out the ones that aren't real, and I'd like to think I've gotten pretty good at it. But am I perfect? Of course not. And so is there one gonna slip through? Well, you know, I try to forward all those to my assistant. So if it slips through, it's gonna be her, not me.

Ieshea: Oh, my goodness.

Robert: A lot of pressure on Tracy, right? You know, but you've gotta, and she's taught me some things too. Sometimes, you look at the email address.

Ieshea: Yes.

Robert: And if it comes from a different domain, somewhere in Japan or Germany or something, well, that's probably not somebody that I need to be clicking on.

Ieshea: Right. So and it used to be a lot easier, but we definitely tell you hover over those links inside of your emails and look down in that lower corner, right? And when you look down there, now, those tiny links have really started, you know, kind of messed that up, but when you can

look in the bottom and you cannot see the name of the company from which it came, I also tell you hover over the name of the person that sent you the email. Because what is being done now too, it comes in and it looks like Ieshea Hollins or Ash, and you can see the name. But when you hover over to the side, then you'll see salesforce@blahblahblah.com. Well, that's nowhere near their email address, right? So now, we know, okay, let's garbage that, right? But again, then it goes back to, so if traditional IT, when you see that, right? And when you, for you to say that you're seeing them every day, that's when I would say that's when an office needs to actually pull somebody in and take a look. Why are you being, you know, and how many targeted attempts are coming through your network, right? Because so now, you need to take a look at, and then in some cases, are they all from the same person? Are these different people, right? And so that's when it becomes important to take a look at what are our network seeing and what are our logs looking like?

Robert: Okay. Yeah, I haven't got time to hover over everything and see where it came from. Now, that's amazing. Yeah, that's amazing.

Ieshea: But, I mean, even myself, I get so many emails a day, same thing. 'Cause, I mean, I'm not just cybersecurity, I'm a business owner.

Ash: Right.

Robert: Yeah.

Ieshea: And so there's so many people that are gonna reach out on a daily basis. Just like this email like, "Let's get together, let's do a podcast," right?

Robert: Who are you?

Ieshea: Who are you? So in this case, we had the beauty of having a connector, right? We had a person that we knew in common that did that polite handshake list. But not always do you get that, you know?

Robert: Yeah, yeah.

Ash: And I wanted to talk a little bit more about what you mentioned earlier that it is possible that you, as a business owner, you may have already been attacked.

Ieshea: Yes.

Ash: Your security may have already been breached and you may not know it. That's kinda scary.

Ieshea: Uh-hmm.

Ash: So there is no way-

Robert: That's shocking to me, you know? I didn't know that.

Ash: And then, there's absolutely no way they can find out unless they employ someone like Ieshea to come in and tell them that, "Hey, you've already been breached." Now, my next worry would be, okay, what happens next? Let's say it's been breached, and a lot of information has been stolen. What can be done?

Ieshea: So with that, what happens there is we will start a remediation process, right?

Ash: I see.

Ieshea: So again, it's gonna depend on the organization. And again, so let's not be completely afraid. And that's the other thing that happens is like, well, if everybody's been breached, well, why worry about it, right? No, let's not do that either. Some of those are just consultations that bring, you know, bring someone such as myself in and we start actually going back through those logs. Let's see how far back does this go. Let's also let's look at the networks that you're on. Have you changed your networks? Sometimes, it's also, when was the last time we did password resets and did any type of scrubs, right? When was the last time we did a cleanup? Sometimes, those are the things that we have to do. But again, it'll depend on what we find once we're there. And we literally in our report can give you back, like a step by step, let's do this, let's do that. And it's not all these, all things have to be done yesterday, right? We create a plan and an approach that says, hey, let's, and we're in this with you. We'll walk through this with you until we get you to the other side.

Ash: Oh, good. And you know, you pointed out something else to Robert that, you know, you getting such emails, that may be a point where you may want to employ someone like me to come in and tell you that you may be targeted.

Ieshea: Exactly.

Ash: Right, so can you tell our listeners some other markers that they can keep an eye out for when that should be an indication that they may be targeted?

Ieshea: Okay.

Robert: Or, I guess, you know, to say it another way, is there anything they can look for that they need to know to be worried about?

Ieshea: So as I said, we're all inundated with emails, okay? So you wanna look for, though, especially if you start seeing emails from yourself to yourself or emails directly to you from your domain that you know could not have come from you. In other words, somebody else has either cloned and, or mocked your own domain. And then, they're emailing you back. So some of this, we would have to literally do a consultation. It's like, I'm looking at Ash and I'm going, okay, I don't know if it's just not clear. I'm probably scared.

Robert: Well, it's just so over our heads, you know?

Ieshea: Okay. So for me, my domain is direnzic.com, okay? So I've literally, and we know, so for us and we'll go through and we'll do a cleanup, so if I see Ieshea sent Ieshea a message, that's gonna be concerning for me, right? 'Cause I know I didn't email myself or maybe I did 'cause, again, there are times you have to email yourself. But if I go there and I click, right? And I'm like, okay, no. So you wanna look for things like that. You, a lot of us, of course, we know what to look for if we start seeing different things that, popups, we've really kinda got away from the whole where, you know, and that used to be a really big indicator, right? So there's popups all over the place. So you're not gonna really see a whole lot of that. You also, checking your, 'cause there's a lot of linkages now between our phones and the network, right? So if you started seeing where there's any anomalies across your phone calls plus your network. So those are things that you wanna, you know, kind of be cognizant of. I'm trying to think what else. Hmm. Patient records that are either, or patients where you're seeing yourself being emailed by a patient, right? And that patient did not reach out to you. So again, now, who you are working with, in other words, they know some of your clients. I'm trying to keep it as low level as possible. I don't feel like that-

Robert: Thank you. Just for me.

Ieshea: I don't know if that was helpful at all.

Ash: No, it was plentiful.

Robert: Yeah, absolutely.

Ieshea: Okay.

Robert: Yeah.

Ieshea: Yeah.

Robert: Well, so what other advice do you have? Kind of in summary because we can talk about this for hours, but I think we're kind of out of time. So tell me, in summary, something you can leave with our listeners.

Ieshea: So number one would be, don't be afraid, right? This is the day and time that we live in, right? Data is king, right? That's what we have to understand. And if you are in charge of any type of data or content that could be of use to anyone, then you, yourself, you are, you're the gatekeeper, right? And so you wanna do your best to make sure that the data you're in charge of that you're doing a good job, you know?

Robert: Well, you have a legal liability to do that.

Ieshea: You actually do.

Robert: To protect that data, yeah.

Ieshea: You do. You do. Yeah, just saying, hey, I'm in business, and that's where my liability stops, it does not. And so get the training that you need. Do not be afraid or ashamed. Get training. And in some of our cases, call for the consultations, right? The consultations may lead to you finding out you do need an assessment. But again, it's just like finding out your business needed anything else. We are no longer at a point, right, you know, we went through that phase where every business needed a website.

Robert: Yeah.

Ieshea: Well, you didn't go back and you didn't look at the website and say, "Well, I can't really afford the website "and so, therefore, I won't."

Robert: I think a lot of people did at the time. But guess what? If you don't have one now, you probably don't exist.

Ieshea: That's exactly right. You have to learn to grow with the times. And that's where we are. So, you know, with regards to that, and in some cases, I will say there are some grants that have been put out, right? We need to start reaching out to our, was it the Department of Energy and the Secretary of Energy, reach out to your government entities and have them to do the research. Because there are so many cybersecurity grants that are out right now to help with those that are saying, "I did not have this in my budget, "but if you can come in and subsidize some of that for me." And when we can start driving enough of the small businesses to say, "Well, I saw that." You know, the grant was put out there because it's actually, one of 'em is called the bipartisan infrastructure deal. It's the BID grant, B I D. So actually start having, if not the dentists themselves, but some of the medical organizations coming together and saying, "Can we find out where those grants are?" And then, once you find where the funding is, then you can reach out to us and go, "Whew, hey, the hard part is done. "Now, we start having those conversations. "When can I get you in to kinda help us out?" And that'll be helpful as well.

Robert: Okay, outstanding. Great information.

Ash: I agree, yeah. Thank you so much for being on our episode today.

Ieshea: You guys are welcome. Thanks for having me.

Robert: Yeah, I'm sorry it was so short. It seemed like we've been here 10 minutes.

Ash: I agree, and I-

Robert: It's been 30.

Ash: And I bet she still has a lot more information too.

Robert: Oh yeah, absolutely.

Ash: So for our listeners who may have questions about any of the content that we talked about, or if you guys need any assistance in this area, please feel free to reach out.

Ieshea: Yes. So our website, again, we are Direnzic Technology Consulting Group, LLC. Website, www.direnzic, right? So that's D I R E N Z I C .com Also, give us a call at 254-244-5533. And my name is Ieshea Hollins.

Robert: Now, does that phone number ring here in Frisco as well? Is this in the home office?

Ieshea: Yes.

Robert: Okay, great.

Ash: Awesome, that's great. And for our listeners that may have questions for us, you can reach us at info@eandassociates.com, and that's and spelled out, A N D. Thank you.

Narrator: Thanks for listening today. Be sure to subscribe to "Beyond Bitewings" on your favorite podcast platform. For more info, you can follow us on Facebook, Twitter, and LinkedIn, or reach out to us on our website. You can also shoot us an email at info@eandassociates.com.