Imani Fields:

Good morning, everyone. Thank you for joining us for today's webinar, Elements of Risk in Construction presented by Rea & Associates, a top 100 regional CPA and business consulting firm with offices across Ohio. My name is Imani Fields, and I'll be walking you through a few housekeeping items for today's webinar. First, if you have any questions during today's presentation, you may enter them into the chat box on your screen. We will try to answer as many questions as we can at the conclusion of today's presentation. However, to be respectful of your time, we know that we will not be able to get to them all. Therefore, following today's webinar, we will review all questions and send out the answers via email as soon as we can. If you'd like a copy of today's slides, you'll find that they're available in the handout section of the webinar dashboard on your computer screen. Today's webinar will be moderated by Doug Houser and Scott Bechtel.

Doug is a principal and director of Rea & Associates construction and real estate practice. Doug oversees the firm's efforts and growth in relationship management for its client segment which is the second largest. Doug's focus revolves around financial reporting considerations and guidance for the firm's construction clients and their third party financial statement users. He also maintains client relationships, responsibility for a number of the firm's flagship construction industry clients. Scott, a principal at Rea & Associates, overseas tax engagements and the related client relationship. He works with clients and industries including construction, real estate manufacturing and service industry. He also works with the associates at Rea to develop them in all areas of their career. His areas of expertise include construction industry tax, multi-state city taxation, leadership development, tax planning entity and individual, and succession slash ownership transfers. And now I will pass it over to you, Doug and Scott,

Doug Houser:

Thank you so much, Imani. Really appreciate everybody joining us. I know it's early and hopefully some of our guest listeners today got their coffee mug and it's already full, or maybe you're on your second cup. Scott and I are extremely pleased to host today and we'll be moderating. Want to remind everybody to send in questions. We're going to have obviously some poll questions as we go for CPE compliance, for those of you that need that, but type in the questions in the chat box there and we will get to those. We want to make this as participatory as possible. It's obviously difficult, we wish we were doing this in person as we typically do, but this opens up some different avenues for us, of course, to get more folks involved and try to participate this way.

So we're going to have a packed agenda here. We're going to run straight through some speakers. We're going to talk about cyber risk. We're going to talk about insurance risk as it relates to construction, state and local tax issues, which I think that'll be super imperative. Look forward to Jones here on that one. We're going to have legal risk, Tom Nocar will be covering that. And Travis Spagnolo from SafeX as well. So he'll be talking about safety and operations and what's going on there. So some great guests today and really look forward to it. And I'm really pleased to welcome Scott Bechtle to our firms. Scott's only been with us now... What is it Scott? Few weeks?

Scott Bechtel:

It's exactly a month today.

Doug:

Oh, month today. So, Scott's a veteran in the construction segment, particularly on the tax side. We greatly value his expertise. So Scott, do you have any opening comments for everybody?

Scott:

I just want to share that I'm excited to be part of the team here at Rea. And as I looked at the list of attendees today, saw a lot of familiar names and look forward to connecting with everyone soon.

Doug:

Absolutely. And just to let everybody know there's going to be a Q&A time during each of the presentations, as well as Q&A time at the end as well. So don't hesitate to do those. So we'll give everybody a chance here to pick up maybe one more cup of coffee. While everybody does that and gets ready, I'm pleased to introduce our first speaker of the day, Shawn Richardson. Shawn is just a super amazing guy, interesting guy to talk to. I always love hearing his experiences and what's going on.

Shawn is a principal at Rea at our firm and he is also a retired US army master Sergeant and former cyber security advisor to the Army Reserves, Cyber Operations group and the US Cyber Command. That is a spooky stuff for sure. So he's got a lot of good stories, but he's also more importantly got 25 years of information systems engineering and cybersecurity operations experience, and he leads our firm's cybersecurity services team. Shawn is committed to helping guide small and medium sized businesses of America down the path of entrepreneurial freedom without the risk of compromise. I love that tagline. So Shawn, with that, we will turn it over to you and look forward to hearing what's going on in terms of cyber risk and maybe you sharing some of your experiences as well.

Shawn Richardson:

Thank you, Doug. I appreciate the introduction. Thank you so much for everyone attending this morning. It's an honor to be a part of this great team here at Rea and Associates. I'd like to start off with one of the reasons why I'm here is exactly what Doug left off with and that is we created something that it helps us identify risk in a dollars and cents, but also from a business perspective for all our small and medium sized businesses. In the cyber security realm of protections and data protections and so on often times the small to medium sized business is overlooked. And on the flip side, a business owner, sometimes he or she doesn't really have a budget for protecting their intellectual property or their customer database or their QuickBooks or whatever the case may be.

So we have a very simple approach and excited to share some of those things with you today. Some of the stories we'll be sharing with you today are real. Most of them are all indemnified, in fact, all of them are. But more importantly, just want to outline what's important in the small to medium size business, more importantly in your segment, construction and general contracting. So where our clients are now, frankly, through COVID we found oftentimes the GC and the construction segment kept going. Right? They stayed at work. And so there were still oftentimes where you'd have remote workers that are communicating through a mobile device, or what have you, and the threat landscape has gone up. So taking advantage of the different open doors, if you will. And when the day begins and the day ends, bad actors or people that are trying to gain information about your company, all they really want is your data.

They really want who your customer database is and they want to disrupt your services. And so what does that mean to you? Your QuickBooks or your backups, or maybe your local server or your internet connection, or what have you. So we'll talk a little bit about that today. Next. So through COVID and even pre COVID, companies are scrambling trying to figure out, "Okay, how are we going to still communicate?" Right? How are we still going to conduct business? Again, construction, I would debate that construction in the general contracting arena still was in business and thriving. But the threats still rose during this time.

So things like a business continuity plan and a desk disaster recovery plan, frankly, are in some cases, nonexistent in companies in the construction and general contracting realm. So we take a step into that realm and help you simplify that process by eliminating the scrambling when things like this happen. And it's no different with any company, frankly, is the lack of expertise. So having a trusted advisor or trusted IT or IT security individual that's within the firm in your firms that you can lean on to fix and or address these concerns. Continuous monitoring, no one really knows what that means.

And what that means is having an advocate, having somebody from the outside, looking in, watch your assets, watch your networks, watch your email, and take a look at different things that could potentially be bad. Right now there's a huge spear phishing campaign going on throughout the world that our security operations center and our partner providers were on a phone just last evening talking through what that looks like. And in just the things you need to look for are what you hear quite often. And that is don't click on unwanted links. Don't open emails that are from people that you don't know, any attachments. And if you follow those rules, you'll be good, and just delete those emails and move on. And then lastly, until now over the last decade, I would debate that cyber security in your realm specifically has really been overlooked and misunderstood. I don't know what that means. Right? So we'll talk about a little bit about that today. Next.

Doug:

Hey, Shawn, real quick. This is Doug.

Shawn:

Yeah.

Doug:

During this COVID time, what really do you think has caused the increase in cyber attack and cyber risk for folks out there? What is the cause of that during this?

Shawn:

Yeah. So a few things, obviously opportunity. So the bad actors that are behind the keyboards trying to disrupt these services and gain access to networks, they now have a new open door and that is your home. Most homes are just not protected like your core networks are within your company. Even the average small business network has some average security controls in place at the base of their network. Right? So to answer your question directly, it's moving that office space to the home environment and that opens doors quickly.

Thanks for that question, Doug. Appreciate that. So let me give you three examples here and just explain what the B word means. We use that in the cyber industry. It is a legal term. And what that means is

within a company if you identified that you've been breached, if you say breached, hacked is used quite often. But that is a legal term. And I just want to put that out there. That means that something has to happen from a legal perspective, some sort of information that is protected, regulated, or a client's personal information, PII, or some sort of credit card number or account number or address or what have you has left your organization. So that's a definition, a very simplistic, definition of a breach.

It's not just an incident or event. So I won't bore you with technical jargon. Okay. But the attack impacts the availability of your systems. So anytime an event or an incident happens, that's in fact what they're trying to do. They're trying to disrupt. And that impacts, that disruption impacts your revenue. Right? So if you're down for a few days or you can't access your GL, your general ledger, that's potentially catastrophic in some cases. So, next. Also one of the things I want to point out from the previous slide is there's a difference between availability, confidentiality, and integrity. So it's called the CIA triangle. Right? So availability is making sure that the internet works, making sure your computer, you have access to the internet, access to all your software. The confidentiality and integrity of said systems, said information on the systems gets overlooked often.

And so that's where your data is at. That's where the identities of your usernames and passwords are. And so those are the two key things that we're looking at. Right? Your internet is going to work or it's not. And if it doesn't, it's either one or two things. It's your internet is down because your provider has a problem or someone has gotten in and potentially gained access to your system and shut you down. So a second example here is theft. And so a breach that actually an access to a system has happened. Information has either left or money has been exchanged. An example would be, oftentimes... We just recently have had several of these happen and that is an email comes in from an accounts receivable or accounts payable email from a trusted, what they think is a trusted contracting company or a partner requesting for a bill to be paid. And in fact, that link goes to an off shore account.

That has happened hundreds of times, folks, just within... This is in the last two years. I can give you insurmountable amount of examples and it's the old adage that you feel like that kid where your wallet has been stolen. I mean, it's just heart wrenching. So that type of theft and fraud is executed through electronic transactions. Next.

Doug:

Hey, Shawn, real quickly, we've got a question from the audience here.

Shawn:

Sure. Absolutely.

Doug:

Increased treats and increased risk that we've got, a question is, do you see software companies keeping up with these developments and attempts to steal information? What are your thoughts on what the software providers are doing?

Shawn:

So, that's an excellent question. So I will say in present modern day, they're getting better. Realistically, from a security practitioner standpoint, they're always behind and I'll tell you why. The threat is so quick and poignant and direct and targeted that there are constant changes to software. Right? And or

needing for someone to validate whether that software needs updated. Let's just use Microsoft as an example because they're easy to use. For years, they've been the bane of our existence because of Windows updates. Right? And in our industry, when a system or a piece of software has a flaw or an exploit, all right, an exploit meaning a break in code or an open door, oftentimes that is referred to as a zero day event. That means there is no patch. There is no fix until the software company fixes it. Okay? So what does that do to your business owner as a business owner?

Right? So you have to put mitigations and have a strategy in place to be able to move left to right and almost like block and tackle until that's fixed. Okay? And so a good example there would be to have a trusted advisor that you can call or on some sort of contract where you can say, "Hey, I need this looked at right away." Or that person's proactive and come and say, "Hey, you know what? That software needs updated. There's a newest, latest, and greatest threat to that software. We need to put a mitigation strategy in place."

Great question. Great question. And so a final example here would be the copy breach. So we're talking about data and frankly, our organization, our success, frankly, has been because as a trusted advisor, we look at data first. It's about your QuickBooks data, your backup data, your customer database, your ERP systems. Okay? How's that data being protected? What controls are put in place that protect that data, because frankly often times you don't even know that they're in. And there's some cases where three, six, nine months down the road is when you actually find out. I'll give you a present day active example right now. As of last month my team basically got in our war room and jumped on a call with one of our clients. It is a school system, and I can say that, and that's it.

But they were compromised and they still are down after six days. So think of not just the effects, the type of vertical there, but bring that over into your vertical. If you were down for six days and had all of your systems inaccessible to include your QuickBooks, what kind of predicament would that put you in? The single largest loss and aggregate worldwide is the copy breach. And that puts a stream hindrance on people's revenue, their brand, brand effectiveness. So yeah. Any questions there, Doug, by chance?

Doug:

No. Nothing on that one.

Shawn:

Okay. All right. No worries. Next. All right, so here's one example that actually happened that we, our team, responded to this last April. It was a ransomware event, small company, about $2 million, well, present day, they were close to $2 million in revenue or an annual sales rather. And a small family owned business, but they were down for 10 days. And it's very rare. And I'll say this openly as a security practitioner, it's very rare that this case here, the data was recovered. So we actually negotiated, our team negotiated with the extortionist and brought the original ransom down from $5,000 to less than a thousand. And the business owner was willing to pay that was willing to risk paying a thousand dollars to hopefully get his or her data back. In this case, the data was recovered. Again, folks, very, very rare case.

But the example that I'm sharing here with you is it took 10 days. It affected their operations. The total operational loss was significant. And so without an instant response team, without a trusted advisor, in this case, it could have been well over six figures and maybe even more downtime. So the things on the right there, these are just things that you should be looking at, implementation of monitoring, testing and updating software. That question Doug had was great. Are you getting reporting back from a

managed service provider if you have one? Training. Training is so, so important, I cannot stress it enough. Controlling access to your databases, controlling access to your QuickBooks. And then how do you take your data and put it in a safe place and destroy it when it needs to be destroyed? And then lastly, do you have a third party trusted advisor that can look at the risk to your business? Okay. So in this particular case, they're up and thriving today. They're doing very, very well through COVID post COVID and it was a success story overall. Next.

Doug:

Hey, Shawn. A quick question here. This is one thing I get interacting with a lot of clients, prospective clients, that the question is, okay, is it better to have all of my data and information in the cloud or on their own secure servers. There still seems to be a lot of discussion around that and the different protections. Some feel both ways on that. So maybe give a little color on those issues there.

Shawn:

Yeah. So that's a great call out, Doug. So movement to the cloud is a trend that's been in place for years. And it's cost effective in some cases, depending on the size of your business. But the controls and the problems and open doors, if you will, that are on premise on inside a business. So a local server is hosted inside a company versus inside a cloud hosted provider somewhere, those controls that you should have in place still apply. So while the cloud is, I would debate a bit safer, they still have to have the controls around it. It still has its own fair share of challenges, Doug. So I would not caution our listeners. I would reach out to a trusted advisor and we can even have a conversation with... Doug and I have had this conversation several times over the last six months and even some members on the team here that we would just have a conversation with you and understand what's your business strategy.

Are you scaling at a rate that it's better off for you to be in the cloud where it's a little bit more cost effective? And by the way, you can put security controls around it and have a trust advisor watching them. Great call out. Appreciate that. So regulation. So I will share with you and a lot of business owners in this space and in small to medium sized business marketplace in general don't understand what regulations apply to me. Okay? So if any of you apply for any government contracts or you're doing state level or federal level contracts, when it comes to construction or general contracting, the CMMC is coming and what that is is a Cybersecurity Maturity Capabilities Model. And basically it's a set of controls that are required for you to even bid on work. So, that's just one example. States, I think we're up to 42, maybe 47 now States have privacy laws and cybersecurity laws of their own. Ohio has a Cybersecurity Safe Harbor Act, which is Senate bill 220 passed in 2018.

And a very easy read by the way, if you want us to send that to you, we can do that outside of this event today. But you can also Google it. It's about 20 some odd pages. But just what it States is if you as a business owner have at least basic controls in place and or a framework in place that controls your and puts controls over your data and protects your customer data and credit cards per GL what have you, and if you were to get breached or compromised, then the state has a safe Harbor in place to protect you from the fines that are coming because the fines are coming. I'll give you an example in the EU and the European Union, they have implemented what's called GDPR, the General Data Protection Regulation.

So what does that mean to you? It's a lot of the flavor that I'm talking about. So I'll put very little color on it. And that is, if you as an individual have an identity, your identity cannot be shared without your consent. And if it's shared and compromised without your consent, then a company that that happened

to can be penalized up to 4% of your annual revenue with one compromised identity. All right. So do the math in your head for just a second for our attendees, would you be willing to give away 4% of your annual revenue as a fine. I mean, so we're going down... I share that as an example. We're going down that path. Okay. New York, surprisingly, they have some really, really stringent financial and cybersecurity laws that they have implemented. And it's requiring business owners down to the small businesses, even sub a million a year to make sure that you have at least a framework or controls in place to protect your company's data and your customer data.

Lastly, during COVID, cyber events have gone up more than 400%. We talked about that at the very beginning. We're bringing the office to the home. Right? So those open doors have brought those threats and those compromises up significantly. Next. So what should businesses be doing now? So here are a few things that you should tackle right away. Before you move your office staff back into your home, you should do some sort of analysis or reentry assessment, if you will. That reentry assessment is something as simple as ensuring that you do a virus scanner or a web scan on the computers to ensure that there's no malware or no unwanted software or open doors on your computers.

Or something as simple as doing a refresh of the software, making sure that there's not any personal data on a company machine that can be sometimes troublesome. And then training, retraining your folks and train, train, train. I can't stress enough. What does a phishing attempt look like? What should you be looking for as a controller, as a accounts payable person, as a general contractor that leads a team of hundreds of people that are in the field that has to communicate with his or her software on a minute by minute basis. How do you identify when something happens with that software or it's inaccessible.

So just different things to look for when you're training. Set very, very clear expectations with your staff and lean on trusted advisors. Having a trusted advisory group come in and having at pull hours, having them a phone call away is extremely important, especially in this segment within construction and general contracting. When we talk about frameworks, I was talking about it already centered around controls, a set of controls that you can apply inside your environment, to your systems and to your business controls as well. Right?

So we're talking about business continuity plans disaster recovery plans, but also tying it back to your business goals and strategies. Okay? Oftentimes there are security companies and trusted advisors that say they're trusted advisors, they just want to come in and sell you something. We're in with one of our clients right now that they called us right away because they're being sold something that is a solution. It's not an advisor. It's not an advisor that is walking them down a path to success. Okay. So just selling somebody a software is not an acceptable framework. And then lastly, go on a data dive. What's that mean? Understand where your data is, understand how important it is and how to protect it.

And then the five things you should be doing right. Know where your critical data is, maintain software updates and patching, continuously inventory your physical assets. That's important. So for UGCs that have mobile devices that are out in the field that are tied back to your home networks. If there's no control in place over that mobile device and it's just out there, it's probably a good idea to bring somebody in to analyze that and take a look at that for you. And it's very simple, there's simple solutions out there for you, and you have likely solutions in place that you've already paid for. Okay? And then lastly, and most importantly, training your employees on threats and routinely, routinely audit the access to the systems that you have. Next. All right. So here's …

Doug:

Shawn.

Shawn:

All right so here's a little bit.

Doug:

Shawn, we've got a quick question here. Somebody's getting text messages on a company issued cell phone from political campaigns, stuff being delivered, packages being delivered. Is that a potential cyber threat, in your view?

Shawn:

So that is a great question. So I will answer that very directly. If you have signed up for some sort of service where you are to be notified when a campaign person is in the area or if there is some sort of event or that you want to be a part of a list of folks that they can reach out to and donate to, if you've signed up for that, then those text messages are something that you allowed. If you erroneously are receiving text messages, SMS text messages, so simple messaging services is what text messages are based on. If you're receiving text messages that you know you did not sign up for or they're unwarranted or unwanted, delete them. Do not click on any of those links. That campaign has been active and running rampant for years.

I'll give you a very scary example. There is a company out of Israel that I worked with for years, they're a firewall company. I have become friends with, through, as security practitioners are, we're a very tight community, we stick together. We want to keep, just like in your community, GC's talk, right? Construction companies talk about, "Hey, those guys are really good. Let's partner with them," or what have you. This company has a gentleman, Mr. Doore, I'll just give you his cyber name, where he caught an SMS campaign, a text campaign where a link gets sent out and if you click on that link, your phone is owned. And what I mean by owned, everything on your phone is being tracked, watched, every click, every single access. You enter your password into your banking app, it's being tracked.

So to go right back to your question, Doug, best practice is to just not interact with any SMS messages that are unwanted or that you receive that come from a service that you think might be something you want to check out.

All right so we're going to wrap up here pretty quick in the next five, six minutes. We've talked a lot about what threats look like. What's an acceptable framework? Should we be doing assessments on a consistent basis? The answer is yes, obviously. So I'm going to give you a little bit about our approach.

So my partner, Paul Hugenburg and I, have been in the firm for about a year. We started a small cyber security firm called the Cyber Six Group and our sole purpose was to service and help businesses like you. My passion as a former leader in the armed services was to protect and serve. And I struggled for a little bit in my time exiting the uniform, how can I take that passion and put it back into America? And I've always had the small business in mind from the very, very beginning. I used to tell my soldiers all the time, don't go to Walmart, go to the local business. Go support your local business. Go have a local company do that for you. That's most important.

Again, my why, our why, is to help you, the small business owner, and especially with our attendees today, in construction and general contractors. So unique hands-on approach. What does that mean? Our approach is we take a very unique hands-on approach. We want to start with a business

conversation. That's so, so important. Often times, I used an example earlier, companies will come in and they'll want to sell you something. I don't want to sell you anything, I want to learn your business. I want to understand what makes you thrive? What are you building that is making you successful? And so we, then, tie that back to a technical conversation and we're still able to size that in a way that is palatable to you, the business owner.

So we build a cyber security roadmap that is aligned with your strategies and growth. We want to grow you and protect you safely. We have a program called the Ignite program. It's basically a very simplistic program for small business owners that we can come in and build you a cyber security program with an information security risk assessment, that's what the ISRA is. And those two together, at the end of that engagement, you now can tell your fellow business owners and contracting companies that you interact with, "Hey, I have a cyber security schedule. Oh, by the way, I have a framework and regulatory controls in place." That's huge. Think about the leverage you could have in growing your business by speaking to that.

And then back to Data First, where's your data? What type of data do you have? And so we have a tool that actually my partner, Paul Hugenburg created about seven years ago. He's very passionate about telling you, the business owner, "Hey, you've got credit card data on that server locally and if that gets owned, this is how much it's going to cost you in a fine. Or cost you in a business."

We're framework focused, so we talked about framework today a lot. That means a regulatory framework that has controls in place. How do you protect the software and the hardware in your business? More importantly, looking at things like in the GC world, you've got mobile devices. Mobile's not going away, folks. And oh, by the way, the threat landscape's not going away. And so there's easy ways to connect into your mobile devices and compromise your general ledgers and your customer databases and so on.

And then lastly, having a consistent assessment. A vulnerability assessment. What's that mean? We're talking about vulnerabilities like we talked a little bit about today, patches, software vulnerabilities, hardware vulnerabilities. People just plug things in and think, "Okay, it works. I'm okay, I'm good." We think I'm secure. Not so much. It takes some massaging. What's going on now? What's actively going on in your environment?

So those are some strategies we have there. Next-

Doug:

Shawn, we've got one last question here as we transition. You talked about assessments a little bit, so can you talk a bit about how maybe a SOC report would play into that? Is that always necessary or can you do ... You ran through a number of different things there that you can do to have that assessment. So maybe compare and contrast that.

Shawn:

Absolutely. So I will share with you, a SOC report, for clarity, for everyone attending today, a SOC report is something that's typically in a publicly traded company. It's required in a publicly traded company. And we have the capability of doing that and there are three levels, SOC one, two and three. It is a regulatory framework that tests the financial controls within the business both on the premise in the business and also external to the business as financial systems are accessed and so on.

The compare and contrast there is we do a risk assessment, we're looking at all controls. So we're going to come in and assess what regulatory body should you follow? So if you're a publicly traded company and you're operating in that space then a SOC report is likely. And what level you're at, we have to ascertain what level you should be at depending on the size.

Other control regulatory frameworks, we start with the NIST cyber security framework. NIST stands for the National Institute of Standards and Technology Cyber Security Framework. So it's a government body that I'm actually a part of, been a member of, have actually provided feedback to the framework through the years and that framework is 106 controls that we have in our system, K2 Compliance, that we can go through. That seems like a lot, right? 106 controls, wow. I didn't know that there's so many subject areas and sub controls that I need to address. Well we've got all that already addressed in our system. We come in and we, again, have these conversations with you, a business conversation and then we turn that into a technical conversation on the back end.

So again, going back to your question, Doug, there are several differences. Another example would be the PCIDSS for credit cards. So PCI stands for Payment Card Industry Data Security Standard. So the payment card industry has a security standard that you must follow. A lot of you, in this realm, have heard of what's called PCI self-assessment. So you self-attest by using some sort of software to say yep, I'm good. I've got all my controls in place, my credit cards are off-shooted to a third party processor, I'm good to go. Not so much. It's important to still have that assessment within your business. We're actually going through several right now with some companies that they didn't realize that we have to perform a PCI assessment specifically because they had so many credit card transactions coming in and out.

So those are just some of the examples. One thing that's often missed in small to medium sized business, and this will be my last example, is HIPPA. So HIPPA is the Health Information Protection and Portability Act. So it's your healthcare. EPHI, Electronic Personal Healthcare Information. Oftentimes construction companies, general contracting companies, small businesses don't realize that they're liable to attest to that as well. Why? Because you have your personnel and your staff's healthcare information in that file that's sitting in your human resources department, right? So if that information is shared, you're subject to a potential audit. Now mind you, very small in scale there because a lot of times you've got less than 50 employees or less than 100 employees, but still there's things you have to follow. So that's a great question, Doug.

Doug:

Thanks, Shawn. Appreciate that. We've got another question or two we'll handle at the end of all the sessions here. We want to move on to Joe and I think we've got a poll question here, correct Imani? We can go to that first poll question. And Joe, while she's doing that, this question came up during Shawn's presentation, everybody can see the poll question there. But this question came up during Shawn's presentation so perhaps you can address it off the top and that was with the regard to cyber insurance, cyber risk insurance and what protections are there and how much more prevalent are you seeing that and what's involved with that? I know you're going to cover a lot of that in your presentation but just wanted to let you know that.

And this is a great question here in the poll. Do you expect your company's use of technology to change in the next year? So I'll be interested to see what folks put here for this. And while everybody is voting, I do want to introduce Joe Urquhart, CPCUCRIS. Specializes in insurance and risk management programs for all contractors, real estate developers as well as manufacturers at Overmyer Hall Associates. Joe

advised clients on insurance issues such as risk transfer, builder's risk, additional insured, professional liability and loss control. In 2018 the Builders Exchange of Central Ohio named Joe the recipient of the BX Presidents Award, celebrating his contributions that have positively impacted the industry. And Joe has been a great mentor to me on the insurance side. When I ever have questions that come up with clients or prospects, he's always the first guy that I call because he's just such a knowledgeable and got a wealth of resources that he can quickly give me a realist and transparent assessment.

Very interesting response here, we've got 80% saying increase in technology spend. I guess probably not surprising but given COVID, I guess a little bit surprised it's that high. So with that, Joe, we'll turn it over to you and I know you'll get into cyber risks, our cyber risk insurance and all of that as part of your presentation.

Joe U.:

Great. Thanks, Doug. Thank you for the kind introduction and thank you again for asking me and our firm to be part of this presentation. We always enjoy doing these types of things. Imani, you may want to next slide, get to my part. We'll go to the agenda there, there you go. And the question that you asked, Doug, just briefly about somebody asked about cyber insurance, that's going to be a big part of the presentation today because Shawn kind of set me up here, got everybody freaked out and educated them on the scary things that are going on in our world, if they didn't already know that. So I am going to speak a lot about just some cyber risks, what we're seeing, cybercrime and then really do a high level review of cyber liability insurance. And then at the end, time permitting, we'll just touch on some different things on COVID risk right now, some of the other things we're seeing in the marketplace. But a lot of what we're going to talk about today ties into what Shawn talked about just a little bit ago.

Next screen. Great. Just all about cyber risk, right? So what are we seeing here locally is what we're going to talk about. And the two things, and again Shawn touched on several. But what we're seeing locally is two, either ransomware or what we call social engineering, which is wire transfer fraud. By far the number of claims that either we've seen with clients or that we've heard about or read about is all related to wire transfer fraud. The insurance industry calls it social engineering, that's just their term but think of wire transfer fraud. Every day I hear a story of someone almost getting hacked or getting hacked so we're going to spend a lot of time reviewing that and that's where the claims are really coming from.

Shawn made a comment that the bad actors are after your data. What we're seeing, because we're more in that middle market space, they may want your data but really what they want is your money. They want your cash. And that's what all this is about. So if you get a ransomware attack, they want your cash. That's it. But social engineering and wire transfer fraud is clearly after your money. So how do you protect yourself? What's those best risk management practices? And we're going to talk about those.

Just quick claims examples that we're seeing, and these are real life, these are real claims situations, is a contractor hires a subcontractor below them to do work. Things are going on, you know the upper tier contractor owes the lower tier contractor money. You start negotiating, there's change orders, there's disputes, whatever. You're emailing back and forth confirming how much you owe the downstream contractor. Suddenly, in the middle of that email string, a hacker, the malware that's on your subcontractor's computer system, they jump into the conversation. They take over the conversation. The upstream contractor has no idea what is happening, they're not paying attention. Suddenly they get this email, "Doug, thanks for this great conversation. Glad the kids are doing great. Just a reminder, we just changed banks so when you go to transfer this $100,000 that we agreed that you owe us, send it to our new bank and here's our routing number. Thanks. Love and kisses to everybody."

Well that's the common thread. Somebody jumps into those conversations and you don't know it and they're telling you to transfer money through an ACH payment to somewhere that's not the proper way. And once that money gets transferred, as Shawn will say, it's gone. It's offshore or it's being transferred, it's gone very, very quickly.

The other one we see a lot is if you're a contractor and you're doing work for an owner. A lot of times owners, depending on who you're doing work for, are not very sophisticated. A lot of times they're schools. Schools just aren't very sophisticated in their systems and their technology and their security. Or if you don't have a really sophisticated owner. Again, a hacker will jump in, start talking to your owner and have them transfer money.

There was a very well known case, this is public information, this happened probably a couple of years ago now. The Cleveland Diocese, Catholic Diocese, was doing a job up in Cleveland. And it must have been a substantial job. They were having conversations with a contractor. A hacker jumped in and convinced, or asked, the controller at the Diocese to transfer over $1,000,000 that they owed to the contractor and they did it. They just transferred it. I don't know if it was a week or two weeks later the contractor called the Diocese and said, "Hey where's our money that you owe us?" And the guy's going, "I transferred it to you, what are you talking about?" And that's how they uncovered that fraud case. Huge, huge money.

The last little example, and this is on a smaller scale but something that you do need to be aware of, it was an employee direct deposit scam. So somebody sent an email into the company saying, "Hey, I just changed banks. Next time you go to do direct deposit of my paycheck, here's my new information." The HR person said, "Hey, we've got to confirm this." Emailed a form back out to the employee and said you've got to fill this out, sign it and send it back to me. This is how sophisticated the hackers are, the hacker had software and was looking for that email to go back out to the employee, intercepted it, took the form, completed it, signed it, sent it back in to the HR person. So very sophisticated stuff and you have to have a lot of checks and balances to watch for that kind of thing.

Just the last thing before we move on, we talked to a lot of our underwriters, insurance companies that provide this type of insurance coverage. Where they're seeing most of their claims, and it's actually in small to mid size companies. Over the years I wish I had, I used to say a dollar but now I'll say $5, I wish I had $5 for every time a company said, "Joe, they're not after us small businesses. They're going after the big companies. The banks and big corporations." And it's farthest from the truth. Small to mid size companies are easy targets. Most of these claims are companies that are under $50 million in revenue and probably under $20 million in revenue. You guys are just easy targets so don't have that false sense of security.

Next. So really, how do you protect yourself, from a risk management standpoint? And Shawn, we didn't really talk to you much when we did our presentations but a lot of this is the same thing. Number one, bullet number one is just train, train, train. How hackers get into your system is when an email is sent into your business and an employee, doesn't matter at what level, clicks on that email and opens up something they shouldn't. It's a link, a form, whatever. That's how the hackers get in. It's interesting. So you've got to train. You can't do it once and think, "Hey I'm okay." It has to be a continual training. Many companies offer software packages where employees can get online and go through some training. They take tests and it's just an education process. Number one is just train.

Then, you've got to make informed decisions. How do you do that? You work with your advisors, again what Shawn said. So consult with your CPA, people like Shawn. That's number one. Make sure you really

understand the landscape, what the risk is, what's going on. Ask your bank. I tell a lot of people that I talk to about this kind of thing, you've got to talk to your bank. When you talk to your bank and say, "Hey, what am I responsible for, what are you responsible for if I get hacked?" You'll be shocked, probably, at the answer. Read the fine print because the bank isn't really responsible for anything. So you think you might have some protection there, you really probably don't. But have that conversation.

Then second, do you have a separate IT firm? Talk to your IT firm, talk about doing risk assessments. What are they doing for you? The only thing I'll say on that too is don't go cheap. If you know more than your IT firm, you need to get a new IT firm, right? I hear a lot of them, they hire these companies, you've never heard of them, it's two people working out of some rental office. Spend proper money, get the proper consulting. Very important.

And then lastly, really is insurance. All insurance is is risk transfer. So after you go through all these steps then you have to say, "Am I still okay with this risk or do I want to transfer it to somebody else?" And that's what you're doing with insurance. So there's many different levels of cyber insurance, which we're going to get into. But I just encourage everybody, as you look at this and work on this, just get a proposal, look at the costs, look at the risk and make an informed decision on whether you should purchase it or not.

So really, we're just going to then get into a little bit more detail on this cyber insurance just so maybe if you do get a quote or you start thinking about it, you're a little bit more informed buyer there. The only thing, a big note here which I hope everybody notes, is that not all cyber insurance policies are the same. It's not like buying a general liability, it's not like buying an auto policy. There's no standard form so they're all different. So you really need to do some due diligence and educate yourself and pick a good policy.

The other thing is don't go with companies that you've never heard of. By selecting a company you've never heard of, the shifting sands of Omaha is probably not a good policy to go with. Try a good, financially strong, reputable company. And then the other thing to ask on that is what else comes with the cyber policy? Many companies offer risk management, website training, breach coaches, all kind of things. So if you're going to spend this money, make sure you're getting the added benefits of a good cyber policy.

So just the levels of insurance here, you can start off, quickly, you've got no coverage. You self insure, going to put your head in the sand and just say I'm not going to address it. Really, you are insuring it but it's your financial statement. Then limited coverage, there are some endorsements now that are coming out by some insurance companies that you can add a little bit of cyber add on to your general liability policy. It's better than having nothing but it is very limited. Might be $25-$50,000. Maybe $100,000 of certain coverages. It's better than nothing but you're not getting a lot, just so you know. Limited means limited.

Then second one, and I talk a lot about this is crime policy. So if you don't go the full scale cyber liability, if you go back and you review your crime policy that hopefully you have, honesty, forgery, protects your cash, you have to include computer fraud and you can add social engineering, that wire transfer fraud. Very important. The only thing there is just know, on the social engineering, the limits that are available are not very robust. So you may only get $50,000, $100,000 maybe a couple hundred thousand at the most. Very, very, very limited. So you've just got to watch that. And then third we're going to talk about cyber liability. Next.

Doug:

We have a poll question. Yes, do you have a cyber liability policy as part of your risk management program? Yes, no or not sure. So be kind of interesting to see, obviously it's become more prevalent, as you discussed, Joe. But it'll be interesting to see what the audience responds on this, whether it's majority or not. Give everybody a few moments to vote.

Interesting. So majority yes but still some not sure. So what do you make of that, Joe?

Joe U.:

Well the 34% that's not sure is a little scary. Now they have something to do when they go back to the office, or make the phone call when they're going back. Of course they're already in their office so they can check that out because they're all virtual now. Interesting response. Interesting response. The ones that actually have cyber liability, the 53%, that's a little surprising. That's a little higher than I thought it was going to be.

So diving into an actual cyber liability policy, we're going to quickly look at some of the things that you should look for and just know what's included in those policies. Again, this overview is just one policy but it's typically all policies are set up similar to this. But again, they're all different so you really need to ask certain questions. So there's usually four coverage parts, or somewhere along there. There'll be first party, third party liability coverage. Very important. We'll talk about breach response and then there's this cyber crime part, very important. And the last section, which a lot of businesses don't think about, is the business income loss. So we'll talk about that.

Next. Next. Great. Liability insuring agreements. I'm not going to go through each one of these coverage parts. I think you get a copy of the PowerPoint. Go back, Imani. Okay, well we'll pop in here. The cyber extortion is very, very important under the breach response. Thanks, Imani. The liability insuring agreements, it's the privacy and security is the first one. That's the liability. So if you get sued by somebody for losing data, losing their personal information that Shawn talked about, you can get sued for that, that comes under privacy and security. That's that third party liability coverage.

Next slide. Then the breach response, just highlighting a couple of these. Again, privacy breach notification is huge. So if you do lose data, personal information, customer information. You need to notify them, you need to protect them. And those it costs, depending on how much data you lose, can be huge. So that's something to know about. And then a lot of these policies, again, will include cyber extortion, which is cyber ransom. You can get ransomware covered. Some of these policies will cover ransomware up to $1 million, depends on the limits that you select but these can be very robust, very high limit types of coverage.

Next. Again, the cyber crime. So if you don't have a crime policy, or if you don't include these coverages under your separate crime policy, you can include them on your cyber policy. So it would include computer fraud, funds transfer fraud. Again, very important. Social engineering, wire transfer fraud so you can get coverage for that.

Next. And here's the last one. This is income. A lot of businesses don't think about this and this is particularly huge for manufacturing businesses or businesses like that. A restaurant, a hotel. If you're out of business because of some type of data breach, like a business that Shawn talked about that was out of business for 10 days. What if that was two weeks, three weeks, a month? You can actually add loss of business income under your cyber policy. Again, that's something you need to really review with

a professional, what kind of limits do you need there? It depends on your business, what you do. But that is an often overlooked coverage that you can purchase on a cyber policy.

Joe U.:

And then just some industry updates, reviewing after the cyber next. Yeah. So I get a lot of questions these days about COVID, particularly from contractors, they'll call and say, Joe, am I covered if a subcontractor claims they get sick on my job site? What if somebody dies and they claim they got COVID on my job site? Take it home. What happens? Those are real questions, real risks. For the most part, it's a bodily injury claim. Your policy should defend you. A couple of things there though, one, they have to prove that they got it at your particular site or your business which is very difficult to do. So just know that.

One thing though, as you review your insurance policies, some policies, and you got to be careful here, will have an exclusion for virus or pandemics. Could be a general liability exclusion property, exclusion. We're starting to see those, some companies coming out with those. So just be wary of that and you should, at all possible not have those on your insurance risk program.

One thing I wanted to mention, and this is so fresh, I don't have a lot of information on it, but the Ohio legislature just passed a law here in Ohio. It's called house bill 606, that grants immunity to employees and businesses that were essential workers for some type of civil action if somebody gets sick from COVID. The governor just signed this a day or two ago. We haven't had a real chance to review it so I can't offer you more than that, but it is something, if you're a business to ask about that, dig into that. I think that's a real nice step to help protect employees and businesses from these types of losses. House bill 606.

The other one, the top one there. Go back. The business income, which was a very hot topic at the beginning, is your coverage for loss of business income. If I'm a restaurant, if I'm a hotel, no, there's not. Most people were saying most, insurance companies, it does not meet the definition of physical damage to a location, but there's been lots of lawsuits since March and April of businesses suing their insurance company and up to this date, most courts are siding with the insurance companies and stating there's no coverage. It's something we're still monitoring, but it looks like that is going to be continuing trend for that.

The last thing just to touch on, because really because of COVID, the shut down, a lot of some of the rules that were passed, employment practices liability. Definitely touch up on that, make sure you have it, be aware of it. There's been a lot more activity in that for many reasons. Could be a wrongful termination, discrimination, things of that nature. Third party coverage, third party claims, and the last one is that wage and hour violation and most EPL policies, it doesn't cover the actual violation, but under an EPL policy, you can get defense costs for wage and hour violations, very important these days. Next.

So I'm going to wrap up just with a quick market overview, what you can expect with what we're seeing. There's been lots said about a hardening of the market and it's, I think, maybe freaking some people out. Not all accounts are seeing this. It's more the exception of what we're seeing, so not all accounts are seeing these issues or significant rate increases. So what's driving that though, if you're a business, if you've had a lot of loss frequency or some severity, that's going to be an issue for you on your renewal. If you are a business with a large fleet, 50 or more vehicles, 100 vehicles or more, particularly if there's some heavy trucks, those are being targeted by the insurance industry and it's all coming back to losses.

They're just getting really hammered with very significant, severe losses so they're focusing in on again, large fleets, large heavy fleets. And again, if you have any loss frequency or severity, you're going to have some issues on pricing.

Umbrella capacity is an issue. Because of these large, severe losses that they're seeing across the country, a lot of insurance companies are cutting back in umbrella capacity. So anything over 10 million, if you have an umbrella over that, you might have some issues on your renewal, either from pricing or how it's structured. So if you have a company that you have a $10 million umbrella this year, your current carrier may say, we only want to do five next year. That creates some issues for your insurance advisor. We can solve that. We just have to go out and get another policy for somebody to sit over the top of that. So you can still get the coverage, it'll just be structured, maybe different, and it might cost you a little bit more. So just something to be aware of.

And lastly is the builders risk, frame projects. For any of our contractors in our audience that are doing multifamily frame projects, just a lot of turmoil right now, a lot of hardening of the market. Capacity is an issue, meaning the number of insurance companies that want to do large frame projects and the rate is going up, big time. So if you get a project that, I'll say over $12-15 million in frame, anything above that, it's a problem now. So you want to be proactive, work early, make sure you're trying to get multiple quotes, even though that may be a little bit difficult, but you just got to be aware, it's a changing marketplace. Next. That's it Doug.

Doug:

Thanks Joe. Scott, we'll let you move forward and get the salt discussion going.

Scott:

All right. As Doug mentioned at the top of the broadcast, I'm a principal on the tax side. In the construction industry, one of the big considerations from the tax standpoint is the state and local tax considerations, specifically here in Ohio where we have all of the unique city taxes and the fun that that brings about. So today to speak and address on the state and local considerations, we have Joe Pop and Sarah Sparks from Rea & Associates. Joe is the principal and the director of the state and local tax services or salt team and is committed to staying on top of all of the state and local tax matters while providing extensive internal and external educational programs in an effort to provide maximum client satisfaction. He is well versed in sales and use tax, federal and state tax audit, choice of entity consideration and so on. Joe earned his Bachelor of Arts from Ohio State University and his JD from the OSU Morris College of Law. He also has the Master of Law and taxation from Capital University Law School.

Sarah Sparks is a senior associate here at Rea & Associates in our state and local practice and is committed to handling tax and legal research related to the state and local tax considerations. With more than five years of experience in the accounting industry, Sarah's expertise includes Nexxus studies, risk assessments, voluntary disclosure agreements, and QuickBooks. So with that, I hand it over to Joe and Sarah.

Joe P.:

Thank you, Scott. It's a pleasure to be with you guys this morning. We've talked a lot to folks in the construction industry over the years and this year, particularly. So it's great to be with you and be able

to share a couple of things that hopefully will be useful for you. So I guess to connect the first two presentations to this one, we have bad guy hackers that are trying to steal your stuff and recover from you. And now we've got the legal side of that, where the government is trying to come and get your money from you. So we're going to try our best to lead you through some of these things, some tips and tricks.

Sarah Sparks is a wonderful asset to our group. She's a senior, she's worked on the ground with some of our largest clients and so she's got, a little later on in the presentation as you see there on the detailed discussion side, she's got some really great case studies that she's going to go through and lead us through. So I'm going to stay up here in the clouds, on the beginning part of the presentation to run through some general high level topics and then Sarah was going to dig down into the weeds and really get into some very specific projects so you can see where some of the complexity and opportunities are.

Also, I should note, there's this timeless battle of good and bad and light and dark Browns and Steelers that goes on. And so as between me and Sarah, we got you covered no matter which one of those you are, we're on top of it. So I won't say who is rooting for who, but we have you covered either way.

Doug:

Joe, real quick, we've got another CPE question we need to do here. So interested to hear what the audience expects here? Company's preliminary expectations for 2021? Down, improvement or flat. I suspect we know what will happen here, but obviously construction, we fared much better than most everybody else through all of this and activity, I know, remains strong this year, but expectations for next year, it'll be interesting to see. So sorry to interrupt but had to get that third one in for this hour.

Joe P.:

Sure. No problem.

Doug:

Down, flat. I'm a little surprised that. I'm pleasantly surprised. We see, certainly the vast majority flat or improvement versus this year. So good to hear.

Joe P.:

All right, so we'll dive into some of the top level, high level things. Just some things that we're looking at. Some of the folks in our community, the state and local tax community talk about when we're doing these zoom webinars ourselves, and that is, there's really two phases of the governmental response to COVID. And you're seeing most of them in phase one right now. And so phase one is primarily a stimulus based, recovery based, kind of phase. And you'll see just some of the aspects that I've highlighted there. We have the PPP loans that a number of clients have been able to take advantage of. We have the stimulus checks going out to Americans making under a certain dollar amount, ADI. Enhanced unemployment benefits. A lot of those provisions there are designed to get a lot more cash into the system and to keep the system going.

And so to the extent that we've seen stable revenue at the state level from transactional taxes, it's because of some of these initiatives where people have been able to retain their job. If they have not been able to retain their job, they've got additional money to continue spending and that has allowed the state transactional tax revenues to be somewhat stable where otherwise they would have taken a

dive. So if you think about it, if you're coming at this from the state perspective, you've got transactional taxes, which are monthly, you have income taxes, which are annual, but maybe people make estimated tax payments. So the first canary in the coal mine is the transactional taxes in terms of revenues not matching up to expectations.

And so we're going to get to the income tax next year and whatever that impact might have to state revenue. How that connects to all of you is of course,,\ if one of your customers is a state and local government, their ability to pay, the timing of the payment and all of that, may be impacted by some of these revenues. And so we do take a look at that and have that as part of our general consulting when you're using your crystal ball to see what's coming up.

Some of the things that the state and local governments have done is delay as many of the filings and the payments. Some of these have just been, hey, we're going to give you a couple extra months to pay in file. And then some of them have really been some dramatic programs like California, who has implemented a long-term loan program on sales tax collection. So it's basically allowed the companies to collect sales tax, that is the state of California's money, and then pay California that money over a longer period of time in excess of a few years, I believe. And so, that's a program that is a little bit more innovative, and we may see some of those continuing phase one programs as we continue on.

I think a lot of us have, if you're listening to the news, you hear a lot about potential disruption coming down the pipe after the presidential election. No matter what outcome that we have disruption is predicted, higher interest rates and things of that nature. And so I think it's important to bear in mind that these phase one stimulus related activities that you're seeing from the state and from the federal government may continue or be expanded in the future. But for now, most of them are underway or completed.

A couple of sort of behind the scenes things that you might not necessarily have heard about or seen or thought about is state-level controversy work. So we work a lot with auditors with the state of Ohio and then States across the country. And what we're hearing from quite a few of them is that new controversy work is being put on hold. And then you'll see there in my last bullet point, a lot of the auditors that are in that controversy space are being re tasked to review refund requests. And so the idea there is that those same auditors that are going to come in and maybe ding your business on not paying the right amount of tax are those same auditors that would review if you think you've overpaid the tax and you have a refund that you'd like them to take a look at and then disperse that money to you. So those are some things that are going on behind the scenes that you may not necessarily have thought about or seen. Hopefully you don't have audit activity that's going on so these things might just be something you're not really looking at.

Let's go on to the next slide. So the phase two government response is primarily in the industry, thought to be a revenue raiser phase. We have increased spending, there will be decreased revenue, certainly from the income tax side of things and then on the transactional tax side of things, with the running out of some of these stimulus programs, it is anticipated that the transactional tax revenues for the state are going to take a dive, and that's, again, a more quick to turn around situation since those are usually filed on a monthly basis.

Due to the proximity of the election and our passive ups observations of what's happening in Congress, it seems unlikely that a federal stimulus is going to happen for the state specifically until maybe January. And when I say for the state, what I mean by that is the federal government has the ability to literally print money. They can do that. State governments typically cannot do that. And so if you're looking at a

state that has been hit hard and has increased spending has decreased revenue, their ability to meet their budgetary requirements is severely impacted. If they get additional stimulus money from the state, that means they don't have to cut programs or increase revenues through taxes, which are really their only other choices. And so it doesn't look like that's going to happen on the federal side of things, at least in the near future.

So again, as I mentioned, phase two is mostly going to be a revenue raising phase. Couple of different things that are going on with that right now. The first thing is a new tax type called a gross receipt tax. In Ohio, we have a commercial activity tax, which is a gross receipt tax. There's about seven other states across the country that have these. Texas, Nevada, Delaware, a couple of examples, Washington and Oregon both have one as well. And these tax types are difficult to deal with because one they're duplicative taxes, they can apply at various times along the spectrum.

So for example, if you've got an iPhone or a widget or something that is going through the stream of commerce, or in the construction industry, a two by four, that is going to be taxed for cat every time it changes hands, unlike sales tax, where it's one person should pay the tax on it, that's it. Just one time. With [cat 00:01:24:35], you could have it at multiple levels as it travels from business to business. So it's a business to business tax. So most tax people will tell you, those aren't really well-designed taxes because of that. It has some unfairness to it. A lot of States, I think there were another 5-10 states, were considering implementing these gross receipt taxes before COVID and after COVID, this is really something to pay attention to, especially if you work in a multi-state environment. And the reason for that being, gross receipts taxes are not impacted by lack of margin. So if you're operating at a loss, you still pay the same in gross receipt taxes. You don't have exemptions most of the time. So it's really a true, if you make the dollar, then you pay kind of tax. So there's a little bit of stability there that states are looking at as a positive. Of course, those have to go through state legislatures so who knows exactly what that environment's going to look like next year.

The other thing that is happening is increased discovery and compliance, particularly of remote or non, in this state based customers. I've got an expanded discussion on that in a minute, specifically to the construction industry. If you're not in a multi-state environment, most of your vendors are. The people that are selling you things are in a multi-state tax environment, and that has impact for you. And we're going to talk about that in a minute.

Mostly for the state, if there's a marching order, the prevailing wisdom is that they're going to go after non-filers, from prior years, that are not in this state base, right? Because that gives them the maximum opportunity to one, recover additional revenues, and two, not harm in state businesses who are generating, activity in the state, sales tax revenue, they're employing people, they got payroll taxes. So the extent possible, they really don't want to ding those businesses, they want to ding those out of state businesses. And we have seen that.

One of the things that we have observed is increased activity from Illinois and from New York City, not terribly surprising, probably with some of the issues that both of those locations have. But these are folks that are getting targeted and it's fairly unusual for our client base to have that audit activity. So it's pretty clear that Illinois and New York City are both stepping up enforcement and discovery on remote companies.

Some other things that states are looking at is removal of discretionary penalty relief. So often if you file a return late, but you paid the tax, you can write in an advisor can write in for you and try and get you out of those penalties. We're seeing a hardening of position there, and an inflexibility started to creep in

on a lot of those requests where they have discretion, they're just not removing those penalties anymore. Same sort of fact patterns, but there's just an inflexibility that's creeping in now because of this additional revenue requirements that these States are facing.

You know, we also have, what I call here, database discovery. So one client recently had an audit with Minnesota. This was a, do you have a filing requirement sort of audit? They responded back with, "Yeah, I think that we've maybe been in business there for a couple of years. Let's call it three, because that's typically what the look back period is if you voluntarily come forward and say, "Hey, I've got a tax issue." And the state responded by saying," Hey, that's great but we have 1099s from people from our state back eight years, so how about the other five years of our, of our filings that you are going to give us? I know you were going to get around to it. And the reason they were able to do that is the states have full access all those 1099 records.

So one quick thing that you guys could do, or you could take back to your financial department is take a little review of 1099. If you've got some of those, have you got them from out of state companies and what the IRS is able to do is to share those with those state tax discovery departments, and so if you have a lot of those, not to say that you necessarily have exposure there, but realize that that could be an Avenue that you might get a letter because of those things, and you may have to then be able to respond with the appropriate responses to try and limit your liability and look back if possible.

Last, but not least is again a reduction in important, but not essential spending. So I have not heard as of yet in the construction community, whether that this has been a huge problem. I would expect that it wouldn't be as bad as it would otherwise be, again,, because of that stimulus activity, that's kept up transactional tax revenues and then income tax revenues aren't really going to hit or be reconciled till next year, sometime that's really when I would expect these sorts of reductions to maybe get more prevalent. Let's go on to the next slide.

Okay. So I do want to spend just a little bit of time here on one of these aspects of discovery that I mentioned just a minute ago, which is remote vendors. And so the background on this is this one slide. I won't spend much time on it, but if you've heard of this case, South Dakota versus Wayfair, it's a fairly important case in the world of state and local taxation. The basic idea here is that for sales tax purposes, states are allowed constitutionally to tax a remote seller, if they just have a certain amount of sales in the state. They don't have to be there. They don't have to be physically present, they don't have to solicit sales in the state, they just have to sell into that state. And that's it. And previous to that, you'll see a couple of those court cases that I mentioned there at the top.

Previous to that, there was still this physical presence component. The states went way down that logical path to the extent that, from what I'm more reminded, folks here that are part of the presentation, they were using cookie Nexus. So if you had a cookie on your phone, because you went to some website, that is physically present in the state, therefore you had physical presence in the state, right? And so it's a bit of a tortured interpretation from what it used to be, which is you have a brick and mortar store, you have an employee in the state, we went all the way over there anyway.

So almost every state that has a sales tax has implemented this rule. There's one or two holdouts. Florida is one of these. And really the only reason that they've held out is because there's a discrepancy or difference of opinion as to which threshold should apply, but all of them believe that this is a good rule. So virtually every state that has a sales tax has implemented some version of this rule. Next slide.

And so here's the question that you might be asking yourself, well, I'm in Ohio. I do construction in Ohio. I'm in one other state maybe, but I think I'm good in that situation. So this doesn't really apply to me,

right? This isn't going to impact me at all. And I think on one hand, it's true. You are going to be in those places that you're doing construction work. You're physically present. You already have payroll tax, nexus, income tax, sales tax, all the taxes right? You're there, you're doing business. There's really no difference in your world between having a big box in a strip center and making sales there, or doing construction projects you have the same sort of situation. But what about your vendors? Let's go on to the next slide.

So let's say that you have a non-Ohio vendor, which is very frequent, very common. They sold you a lot of things and they haven't charged you tax. You owe this tax, right? As a construction contractor, for the most part, either you or your subs, whoever is doing the install work in the construction contract rule that, Sarah is going to be talking a little bit more about that, along with some of the exemptions for specific industries in one of her examples. But generally speaking, as a construction contractor, you owe the tax for materials. And so if you have an out of state vendor who hasn't charged you tax, you do owe it to the state of Ohio if the project is in Ohio. Maybe you paid it through use tax, and maybe you didn't. Here is how the Wayfair case has impacted folks, many of our clients in the construction space.

And that is that vendor either gets audited by the state, talks to a consultant and figures out what their true risk is and decides they need to get right with the world. And so they come back to you and they say, "Hey, we've sold you X number of widgets over the past three years. We need you to pay us back taxes in this amount." It's usually a big number, right? A lump sum. And so you're faced with a couple of not too savory choices. The first is, okay, well, you pay it. So this is a situation where Wayfair really has impacted you because you didn't pay use tax in the first place, your vendor is getting caught by it and now you're having to pay that tax. So that's unsavory choice number one.

Second choice is you refuse to pay it. You say, "you know what? That was your decision to not charge me tax. I'll tell you what, I'll pay it going forward, but I'm not going to go backwards. I'm not going to pay you that." And a lot of people do that. A lot of folks, when we're doing this for these kinds of projects for those sorts of vendors, the customers say that all the time. I'll go forward, but I'm not going to go back. The issue with that is most of the time these remote vendors are going, and they're doing these voluntary disclosures with the state. And as part of that, they have to give up their list of all the customers that they didn't charge sales tax to, or who wouldn't pay them now, and they have to disclose that to the state as part of those agreements.

So you might refuse to pay it, and then you might get disclosed to the state by your vendor. So that's not really a very favored choice either because that could end with you being audited. You could pay it again if you've already paid use tax. So many times they won't accept use tax filings, or you don't keep sufficient records to show the tax that you paid was specifically for this, right? It's a lump sum that you pay on use tax or sometimes we sometimes advise clients that just don't want to deal with that complexity to just do a percentage of a purchase account and send in a use tax amount there. And if you do that, you're not able to say that you had use tax to a specific vendor and that's troublesome as well.

The last is you could give an exemption certificate and most of the time, absent some of the specific examples Sarah is going to go through in a minute, you don't really have exemptions that apply to you in the construction industry in Ohio, for the most part, unless you're dealing with specific industries. So that's just a couple of quick, high level things. I know I want to be mindful of time so I want to turn this over to Sarah because I think that was my last slide. Yes, okay. And so hopefully that's somewhat helpful. We're doing work in a lot of areas here to help businesses out. Sarah's got some really great examples so I'd like to turn it over to her. Whether she's for the light or the dark, I'll let you decide, but go ahead Sarah, take it away.

Sarah:

Thanks Joe. Okay, so I just wanted to start off with a case study here for a project that we worked on with a general contractor who'd won a bid with a large manufacturing company to build their new manufacturing facility here in Ohio. And we just assisted them with some of the sales and use tax challenges that they were facing with that.

Just a little bit of background on who the different players were in this manufacturing facility build project. So we had the general contractor who, in addition to being the GC, they also provided some of the asphalt and concrete construction services during this job and we also had some of the general contractor's subcontractors who provided services like electrical plumbing, framing, roofing, and HVAC. And finally, we had some vendors that the general contractor was using to purchase and install furniture, signage, and manufacturing equipment.

So the general contractor and their manufacturing customer had reached out to us in the assault department here at Rea, to provide some sales and use tax consulting services, just to make sure they were paying sales tax where they needed to and were getting exemptions from sales tax where they were due. Next slide, please. Thank you. So some of the things that we did to ensure this were we reviewed the general contractor's invoices that they sent to the manufacturing customer and their blueprints of the project to see where the manufacturing process began and ended and what purchases fell within this process because the manufacturing process, which is generally exempt under Ohio's rules for sales tax purposes, was where we were going to find important exemptions from sales tax for both the general contractor and the manufacturing customer. We also identified some items such as the new facility's truck dock equipment that fell outside of the manufacturing process, which Ohio considers to be taxable, tangible personal property instead of real property after it's installed. And then after our review, we provided the general contractor with our determinations of which items in their invoices and blueprints were exempt from sales tax and which items needed to have line items of sales tax added to the invoices that the general contractor was sending to the manufacturing customer.

Now to ensure the general contractor was able to reap the benefits of the manufacturing exemption, since the exemption needed to be passed through from their manufacturing customer, we created and provided the general contractor with a resale certificate that they could in turn, give to their vendors and subs for the parts of the job that fell within the manufacturing process and included tangible personal property that would otherwise be sales tax taxable, if it wasn't being incorporated within the manufacturing process. And then we completed and provided the manufacturing customer with an exemption certificate for the manufacturing process for this job that they signed and provided to the general contractor so that the general contractor could support their position of not collecting sales tax from the manufacturing customer on the related equipment for the manufacturing process.

Next slide.

So our overall goal here was to work with the general contractor and their manufacturing customer to save the general contractor money upfront on their purchases that may have been exempt under Ohio's manufacturing exemption so that they could then pass those savings on to their manufacturing customer. We also wanted to help protect both the general contractor and the manufacturing customer in case either of them were ever audited for this facility billed job for sales tax by Ohio, making sure they had sales tax line items on the equipment purchases listed on the invoices that Ohio considers taxable and so that they had appropriate exemption certificates in place on the items that were exempt because of the manufacturing exemption.

And then finally, it's always our hope that construction contractors can take the knowledge that we provide when we work on these projects regarding what purchases and sales for their customer jobs are taxable and which are exempt so that they can apply them to future jobs and hopefully win more bids at lower costs.

All right. So I'm going to try to power through this one, unless-

Doug:

Hey, Sarah, my apologies, since we're running a bit behind, can we jump to the to do list? So we try to keep on track a little bit? We do apologize that we're running a few minutes behind, but we will certainly do our best to get this wrapped up by 10:15 as promised. So to do lists are very important questions. I want to make sure Sarah has time to go over these. So, thanks.

Sarah:

Yeah. Perfect. So our takeaways today, we've listed some questions that we're hoping you guys are thinking about. So the first of which is where do you have nexus? And if you have nexus in states or cities, are you currently filing in these places? How are you managing the difference between real property and tangible property status jobs or portions of jobs? So that goes back to the case study that I just talked about, where we should be reviewing if there's anything that should be exempt or anything that should have sales tax line items added to the invoice. And then how are you documenting these exemptions? Are you providing exemption certificates to your vendors and subs? Are you collecting them from your customers where applicable? How are you tracking your use tax on items you may be buying exempt? What software or procedures do you have in place to assist you with bidding on jobs, collecting exemption certificates, or tax and defending a possible future Ohio tax audit?

And if you're buying or selling either most of the business assets of another company or the company itself, have you considered any latent SALT issues? And then finally, which we weren't able to get to, was the discussion about transient workers. If you have workers that work in multiple cities across Ohio every day... They don't have a regular workplace they report to... You guys can go back and reference my slides. I have pretty detailed slides there, and you can also always reach out to us with additional questions. But the question here is for transient workers, are you always withholding city income tax for every day that they're doing work?

Joe P.:

On that really quickly, we could spend hours talking about a lot of these to do list questions. Most of the time, these sorts of issues are pretty easy to spot. If you're in your company's finance department, accounting department, you can ask yourself and some of your teams some of these questions. If you're not, if you're a business owner, you can go to those folks and ask them some of these things. For the most part, we've found that companies either have no controls or the controls that they have really aren't adequate or they're outdated. They're good for five years ago, but there's a couple of things that have changed since then. And they need a refresh and an update. So similar to the cyber policies, it's either you're good, which is fairly rare. Two, you don't have any controls. Or three, the controls you have could use a sprucing up.

Particularly with the municipal tax thing as Sarah mentioned, there was a recent law change a few years ago that if you haven't really accounted for that, it's very likely that you've got some issues. So we're here to help. As needed, reach out to us and we're glad to have a conversation.

Doug:

Okay, Sarah, a quick question that we earlier in your part of the presentation, in the case study, did the GC have to make a sales tax account just for the purpose of charging sales tax on that particular project?

Sarah:

So when we worked on that project with them, we did tell them that it was in their interest to make a sales tax account for super sales tax. But they opted to do this back door type of thing, where they just had the vendors charge them sales tax, and they charged it back to the manufacturing customer on the things that were taxable. And this isn't something that usually holds up under audit, but the way that they broke it out on the invoice is they took the cost of the items that their vendor charged them. And they broke it out with the sales tax that the vendor charged them on the invoice to the manufacturing company. So that's one way to do it. It's not the right way to do it, I'll have to say, but that's the way that they wound up doing it. And they are still without a sales tax account.

Doug:

Awesome. Thanks, Sarah. We have one full question here before we transition over to Tom. So company's most significant areas of risk among these choices. A great question here. So we'll be interested to see that answer.

While folks are doing that, I will introduce our next speaker, Tom Nocar, who is a senior attorney in the litigation department at Porter Wright where he co-chairs the [construction practice 01:48:12] group, with over 26 years of experience. Tom, he's in construction management and real estate development. He's got a unique combination of skills. There's his broad technical knowledge of the commercial construction industry with a practical approach to dispute avoidance and resolution. And quick story, tom also ran his own construction company for a period of time, too. So he's a valuable resource in that he has been on both sides of the fence, obviously, and got great perspective because of that. So with that, we will move on to Tom's presentation.

A little bit surprised at the areas of risk assessment that our audience responded to there, very interesting. So with that, we will move on to Tom.

Tom:

Well, good morning, everybody. Doug, thank you very much for inviting me and having me on this program. If we can go to the next slide.

So this is the question I want to pose to you when we first start out. What do you think the number one way to avoid risk on a job site is? Next slide.

Know your contract. It's that simple. So I saw 22% of you hold, thought that legal and contract was your issue. I'm here to talk about that today. I going to try to give you a couple tips on how to avoid litigation because really it stems down to just understanding how disputes develop. Sean talked earlier about his, why. Why he does what he does. Why he's motivated to protect.

Well, as Doug mentioned, I was in the industry for 27 years before I became an attorney. And so my why is, I can't stand bad actors in our industry. Can't stand them. And I love punishing them. So, but that's not how all disputes start. Some of the disputes start from our control. Your control is what you agree to do under your contract. So what, the purpose of this discussion today is to give you what I view as the top terms that you need to absolutely pay attention to when you are drafting a contract or agreeing to a contract. All right. So let's start with the next slide.

Okay. We have a poll. I'm curious, who's listening? So if you wouldn't mind answering this bullet, it would be fantastic. While doing that-

Doug:

I thinking we'll have a good mix here. It'll be interesting to see.

Tom:

Yeah. While you're answering that, I'll tell you this. The disputes generate from one or two areas, either the bad actors or just miscommunication and sometimes both. But most of the time it's one of those two, and it becomes very clear and evident quickly to those of us who litigate construction cases and for those of us who draft contracts.

Okay. I'm in the office and I run... So some field folks, no designers, a number of owners and a number of folks who work in the office. Fantastic. We'll make sure we gear to that because we don't have a ton of time. I've got to cull this down a little bit. As Doug mentioned, we're running a little long, so let's go.

So the honorable mentions, these are the ones that didn't make the top 10. And I want to talk a little bit about them because you need to be knowledgeable of them. The contract entity... What do I mean by that? Well, in any litigation, well, let me just start with this. Whenever I draft a contract, I feel like I'm writing my opening statement. And so I want to make sure that that contract includes someone who's collectible and make sure it includes the terms that we are implementing in the field. So the contract entity, believe it or not, this gets overlooked an awful lot. Who is, who are you actually contracting with, doing business as? Is it spelled correctly? Are they actually a great company? Is it a sister company where there's protections from the mothership, those kinds of things. So understanding who you're contracting with is important.

Whether or not there are liquidated damages. Liquidated damages generally appear. You see them often in public contracts. Sometimes you get them in private contracts, not as often. And they result from, for unforeseeable damages that are difficult to calculate and they have to be reasonable and proportional. So if you ever get a liquidated damages term and you feel like it's exorbitant, you go ahead and HIO and you go ahead and just call that out and make sure that you agree with that number and that it's attainable just to your work, not to the overall construction project.

Termination for cause or termination for convenience. Generally, you'll see a termination for cause. You don't necessarily see a termination for convenience. But when it appears, it basically gives the contracting party the opportunity to just cancel the contract at any point for no reason. And there are certain things that you can collect and certain you can't, and so I would make sure that you get that looked at as well.

And of course, prevailing wage rates. And these are public projects. When you have... Classifying your workers properly, making sure you're paying them properly. These are important terms.

All right, let's go to the top 10. So I'm doing them in Letterman order to keep your intrigue. But the first one is attached, that Number 10 is Attached Exhibits. So every contract eludes to Exhibit A, exhibit B, Exhibit C or something along those lines, or it makes reference to the Owner's Contract. And there may be flow-down provisions within that contract that you have to take responsibility for if you're a subcontractor. Or how about your proposal? You think you're submitting a proposal and that is what's in the agreement, but contracts typically do not include proposals. And they certainly don't want to have your proposal terms in them. Sometimes they include all of your scope of work. Sometimes they don't. Sometimes they add scope of work that you didn't propose. So it's important that you make sure you understand all the attachments that are included with the contract, the schedule, the drawings and specs of the latest drawings, the latest schedule. There's several. Next slide, please.

This is just one page from an actual contract that I've looked at and there's a second page to it. I think it went up to Attachment X. So you are contractually responsible for each and every one of these attachments as they relate to your contract. So if you haven't read through them, you're exposing yourself. Because when they give them to you and you look at how they play within your contract, you could find yourself accepting some liability unknowingly. I consider this a miscommunication because it really takes an awful lot to go through each and every one of these documents. And you well know that, but if you do it right and implement it in the field, you're going to stay out of court.

Next slide, Number Nine, Attorney Fees and Costs. Yes, I bring this up because it is the biggest issue I deal with with clients. No one wants to spend money on an attorney to collect monies they are due rightfully and I... It pains me to be involved in those situations because I was on that other side of that fence. And I realize how it eats into the profitability of a project. We try to pay attention to that upfront proactively. Are attorney fees allowed? Is it only one party that gets them? I've seen those provisions. Is there a Prevailing Parties term within the contract? How do you determine who prevailed? If you win a little bit did you prevail? If you both win something, did you prevail? So we make sure we have terms that take care of that.

And then Conditions to Collect. What's it take in order for you to actually collect attorney fees? Now I will tell you... And I'm sorry back, yeah. The American rule is what normally applies. If the contract is silent, then each party is responsible for their own attorney fees. Okay, next slide.

Number Eight, Dispute Resolution. Okay, I know this seems litigation heavy right now. I promise you, we get to the things that... These are things that I pay attention to because I want to make sure you collect as quickly as you can. I want to make sure that we remedy the matter as fast as possible. And there are steps that have to happen in order for that to take place.

You may have a requirement to negotiate, even though you want to file a lawsuit, you may have a requirement to mediate, even though you want to file a lawsuit or arbitrator. So there's... Each of those steps have to be run in order for you to get to the next one. If you need to know more about that, I'm happy to discuss.

So Venue and Choice of Law, where must the lawsuit be brought? Is it in Texas? What that means is what's that going to mean to your attorney fees? It's going to be more expensive for you to litigate a case and all the witnesses are here in Ohio and you've got to get them to Texas for court. You want to make sure we guard on that. Generally, the rule of thumb is wherever the real estate is, is where the venue is.

And then Choice of Law. Of course, that would be, you'd want Ohio law to prevail. And generally, as I said, the rule of thumb is unless specifically contracted else wise, the choice of law resides in the state where the property is.

Let's go Number Seven, Notice of Claims. I know everyone out here has heard about this. And so if you failed to provide the proper notice, you've essentially waived your claim. You see it a lot. You see it with mechanics liens. You have 75 days after your last day of work to file a mechanic's lien. If you don't do it by then, your lien rights are gone. If you don't file a Notice of Furnishing or Notice of Commencement, or if you were the contractor and not in privity with the owner, if you're the subcontractor, you need to file a Notice of Furnishings when you start your contract. It notifies the owner that you're out there.

And if you don't do that, and there's a Notice of Commencement, you don't have lien rights. So notice of Claims is important. Generally it may tell you, you have 14 days, seven days, I've seen 28 days, I've seen three days. How long you have from the occurrence to the point where you have to notify them that there's a potential claim.

Next, you have to put it in written... No, I didn't mean next slide. Can you please, yeah. Does it need to be written notice? Usually it is. Verbal notice is generally not enough. An email is a writing, as long as it has the components of that notice. Timing of the notice that we just talked about and you can wave it.

Number Six, Insurance. Joe spoke a lot about insurance. By the way, like Doug, I also go to Joe for insurance, when I need down in the dirty and depths of insurance, Joe's the guy. But anyway, when you're judging your insurance, sometimes I've seen the limits massive. I've seen them standard. Whether or not you need to provide them a deck sheet, things along that line, it comes down to your risk tolerance, what you're willing to accept. So understanding the limits, understanding the coverage, whether or not it's an insurable event. We had... Joe will tell you plenty about that. You probably already know. A subcontractor's defective work is no longer covered under the general contractor's insurance. But there are riders that are available through insurance companies to make sure that it is so you can protect yourself. And I would recommend you talk to Joe about those situations.

And then whether you have any liability for non-covered events and whether or not there's a bond. All of these things appear in your contract. And you probably know this. My recommendation best practices is you take that section of your contract. You send it to Joe and say, or your insurance company and say, "Do we meet this?" And then take that out... You don't have to think. They know.

Let's go to Number Five. All right, Number Five is Indemnity, whether or not you're agreeing to pay the losses of another party. All right, next slide. Next slide please.

So talking about indemnity, what you want to do in that is limit your risk of liability. Some indemnity clauses are very broad and others are very, very narrow and there's some intermediate in between. you're looking for neutrality. So if you're indemnifying them, they're indemnifying you. You're looking to indemnify only work that you control, not necessarily work that they've performed negligently or either any of their other contractors. Narrowing the scope, omitting the acts of indemnity, which is not making yourself responsible for the work of others, and whether or not you can recover legal fees when you are brought into a case that you're indemnified of.

So let's go to Number Four. Now we're getting into what I view is the practical side, the meat, Change Orders. Probably the number one cause of disputes are from change orders. And so understanding the change order process is very important. It varies by contract. Some don't. If you're doing a state contract over and over and over again, you understand the process and an Article Eight and how to make a claim. But when you're doing private work, sometimes contracts are silent to it and they shouldn't be. But a lot

of times there's, basically changes need to be in writing, rule of thumb and you shouldn't start the work until you have that writing. You and I both know that doesn't happen in a lot of cases. And that is the genesis of many of the misunderstandings and the opportunity for bad actors to really be predatory to those who are good actors. And I can't stand that. Okay.

Anyway, Change Directives, whether or not they have the ability to order you to do a change order. What is the type? What is the pricing process for change orders? Is it a lump sum, itemized cost plus, or anything else? What backup do you need to prove it and the require? Do you have to extend your bond or your insurance is another? What's it take to get a change order approved? And how do you get paid for them? How can you bill for them? What do you need to go through? If you need a signed off change order before you can even bill for it, you surely shouldn't be working until you have that signed off change order. Let's go to the next slide.

So Number Three is Schedules. So many times there are schedules that are provided in contracts. Some schedules are way better than others. Sometimes it's just milestone dates. What you're looking for is clarity here. You want to make sure that you understand the schedule. That they're reasonable durations for you to perform your work. That the timeframes that are provided in there are as you bid them. I would encourage you, as you put proposals in, that you include, [temporal 25?18] Information saying, "We plan to start in April. We're going to be there for a month, and then we're out. And we're going to look for payment in July or June," or whatever terms you want. But make sure those timeframes are in your proposal. And then make sure they get into the contract. And that it integrates with the other work that's going on around you so you're not prohibited from doing your work performing.

Let's go to Number Two, Scope of Work. Believe it or not, this is amazingly one of the... "I don't have that." "Oh, well I told him that in my proposal," and there's the contract and it's clearly not there. So you want to make sure that you review that scope of work. Don't just take it for granted that they included everything in your proposal. And you want to make sure it's the five C's. It's clear. It's concise. It's complete. It's correct. And it's coordinated. Next slide please.

So for instance, these are some examples where I've seen items pop up within a contractor's scope of work that they didn't bid: temporary utilities, crane or hoist. Who's responsible for getting the materials up to the floor? Whether or not you have a lay down area, whether or not you have parking. What needs to be done? Whether or not it matches your bid. What qualifications or exclusions that you gave them with your proposal. Are they in there? Do you have access to the work? And what other special site provisions? All of these... This is just the scope of doing a building. It's outside of... Let's say you're a plumber. It's outside of running pipe. It's outside of the inspections, but it's all necessary for you to understand and it makes you profitable. The more time you spend on trying to get materials to a floor, the less money you're making, or any of these items.

All right. Number One.

Doug:

Tom, before you go ahead we've got a question here that I thought was interesting from one of the audience members. An owner of one of our projects attorney added contract language to an AIA asking us, being the GC, to voluntarily and expressly waive immunity, granted under the Ohio Workers' Compensation Act. Is that legal?

Tom:

Generally, no. You cannot contract around the law. That's that's the short answer. You can contract around waivers, but only in certain, not most conditions, but there are some Acts that do not allow that. It seems to me, waiving immunity would be... I'd have to look it up with you... But I haven't studied that particular Act very frequently, but I would, the rule of thumb is your instinct is correct. It's probably illegal. And frankly, if you agreed to it and it went to court, we would argue that it's an impossibility because it's illegal to contract around the law. Okay?

Let's go to Number One. Of course it's payment. That's that's why we do this. We love seeing the wonderful buildings we've accomplished and the wonderful quality, and providing paychecks to everybody, and just having that pride in our work. But the bottom line is we've got to get paid to do it. And so the key about payment terms are you just want to make sure you understand them. You want to understand whether or not there's any kind of initial deposits. Whether there's a progress payment and how frequently you get paid. Whether or not it's milestone, instead of a progress. Whether you get paid for stored materials. How about special materials you have to buy up front? Supposing you're putting in a massive air handling unit and it's got a three month lead time. You want to get that paid up front. So you want to state that in the contract. This is what I'm going to do and you make sure to get you get paid for it so you have something to rely upon.

When can you collect retainage? Again, for instance, my site work contractors, they're done before the job's even 50% complete. And the retainage gets held til the end of the job, unless they get some reduction put into the contract that it allows. And it takes the general contractor to have that in his contract with the owner, as well as you, the subcontractor, having with the general, that they're able to draw 50% of the retainage at 50% complete completed.

And then final payment, what do you need to submit for final payment? I've seen some outlandish and very difficult provisions that require literally everything, and some things out of your control, like an owner sign off on a punch list. You can't make an owner sign. But meanwhile, you're waiting for your final payment. So it's... So the invoicing requirements are very, very important within your contract and making sure that you understand those. All right, next slide.

All right, so here's the top 10. I think we have a poll question.

Doug:

We do. And Tom, we've got one other question for you while folks take a look at this. I love your top 10, by the way. And couldn't agree more particularly at the top of the list, the scope and payment. But question from the audience came up. Can a GC refuse to pay signed change orders?

Tom:

Oh, well obviously I'm going to give them the legal answer. That depends. If you have a signed change order, you better have a good reason offset, or they may have breached the contract already. You don't have a responsibility to perform your promises in a contract if someone else has breached prior to you. There's a litany of reasons why not to pay. But I would say generally you should pay a signed change order unless you have mitigating circumstances that preclude you from doing that or give you the right to withhold the money.

Specifically, let's just say this. You're asking me, "Should we pay a change order?" The reality is, did they perform the work? You know what I mean? If they didn't perform the work, no. So there's a lot of

answers to that. I'm happy to discuss. I'm glad to see most of you agree with me as to payment being the number one. I'm curious as what that 11% of the others are. So if you want to send something in or send me an email, I'd love to discuss any of this with you. That's what I have today. Back to you, Doug.

Doug:

Thanks so much, Tom. And I've got the disclaimer up there as well. Tom's got great insight and great experience. I always love hearing his stories. So appreciate that. And with that, we will move on to our final presenter today, final speaker, Travis Spagnolo of SafeX. Travis is a safety specialist there. SafeX is an EHS consulting firm located here in central Ohio. He specializes in onsite construction safety audits, safety training, and supporting manufacturers with their EHS goals. Travis is experienced in delivering toolbox talks, developing job hazard analysis, and is a training facilitator for fall protection, scaffold safety, lock out, tag out silica, confined spaces and various other safety and health topics. So this is something we should all obviously pay close attention to. And Travis, with that, I will turn it over to you and we will, for the audience, we expect to wrap up at 10 20. So that's when we will try to end for everybody. Thanks.

Travis:

Thank you for the introduction there, Doug. Good morning everyone. How's everybody doing this morning? My name is Travis and I am a safety specialist here with SafeX. Next slide please, Irani. We can get going right into this. So I am not here to talk much about the Coronavirus in particular. I think at this point in time, everybody's kind of all talked out about the Coronavirus, but what I would like to do is share some ideas and thoughts regarding how we can continue working in the construction industry during a pandemic. So again, my approach here is not to push any views or opinions on anybody. I think by this point, 6 months into this, everybody has their own beliefs, ideas and views about the whole Coronavirus pandemic. So my approach to this is just giving you things that I have seen on job sites and giving you just some insight and recommendations to keep your people working safely.

And then even if you're not out in the field working and with boots on the ground on site, if we have people who are still out there working, we all have jobs too. So, kind of look at it from that perspective. So again, there's a small bit of regulatory information that I want to talk about regarding respiratory protection. There's some confusion when we look at like mask mandates and things like that, when that has become a state and local thing, a lot of the general contractors have started to require them as well, even before the mandates came out and things. So we'll talk a little bit about that. And then again, I'll talk mostly on some recommended actions that you guys can take as an administrative perspective and administrative policies and then onsite as well.

So next slide. Next slide, please Irani. So I don't need to talk too much about this. I think by this point, everybody knows how COVID-19 and other viruses for that matter, how they're transmitted and how they're spread. Ultimately we've learned with Coronavirus, the primary transmission is through respiratory droplets. So when you're talking, you're coughing, you're sneezing, things like that, you're creating and you're spreading these microscopic droplets. And that just happens all the time, even when we don't know, and we're not spitting and we're not trying to produce any of those droplets. They're always coming out of our mouths and out of our noses and things like that. So previously what we thought back in March when the whole pandemic was first starting and we were first learning about it, everybody thought that the big way of spreading the virus was the surface to touch transmission.

So you would touch something that had the virus living on it, then you would touch a mucous membrane, whether in your eyes, your nose or in your mouth. And that's how you would contract the virus. That's still possible, but it's not as likely what we know now, as far as the way it's spreading through the air and through respiratory contact and things like that. So previously, when you looked back at all the grocery stores, they were out of disinfectant, wipes, hand sanitizers, things like that. It was just how we were looking at what we thought was the primary method of transmission. And now with the mask mandates in a lot of States and local governments have put out and things like that, that's part of the change of how we're approaching and how we're trying to combat the whole pandemic. So next slide please.

So I'm going to start us off with a quick poll question. I'm going to let you guys see these pictures real quick. Can you go back to that real quick Irani? For those of you might not have caught it. We've got a surgical mask, a cloth based covering, then an N95 respirator. So the first poll question here that we're going to ask is, which of these is best preventing the spread of virus. You can go ahead and throw the poll up there.

Travis:

Okay. All right. I'm adaptable. That's not a problem. So the correct answer for what is going to prevent the spread of virus for that, if you did not have a chance to answer, it is actually going to be the surgical mask.

Okay. So just to make very clear here, the N95 respirator and the cloth face covering, they do about the same in terms of effectiveness as preventing you from actually spreading and passing droplets onto another person. The actual medical grade surgical mass, which is a picture you see on the left there, that's rated for spittle, it's rated for respiratory droplets in very close proximity. So typically depending on the brand and the style of the surgical mask that you're getting, it's either a two or three ply style of paper and material and things. And that's what's actually preventing the droplets from going from you to another person. So even you think back to pre Coronavirus, and you think back to when you went to the dentist and things like that, the dental hygienist and the dentist that you would see and things, they would always be wearing the surgical mask. And that was really the whole point of it. It was not to provide any protection for themselves. It was prevent them from spitting on you and passing on any of their germs and droplets and things onto the patient. So the next question would be, of those same things, which of these is considered a form of personal protective equipment? You go ahead and throw that poll up there, Imani.

And again, when we talk about a form of personal protective equipment, we're looking at something that's actually providing protection for us, not necessarily something that's providing, you know, it's helping to stop you from spreading to something else, but what is actually preventing you from getting injured or from getting sick, things like that. A lot of times we're trying to use terms interchangeably and things, but it's very important to understand what an actual item of PPE really is. It's really designed to protect you as an individual. So for the 71% who said an N95 or professional grade medical mask, that would be correct. It is a form of personal protective equipment. The surgical mask and the cloth based coverings, they are not designed to protect you as the individual wearer, they're not providing any level of protection against droplets coming into your breathing zone.

If you're wearing a surgical mask or a cloth based covering and a person that you're right next to is not, then you can still breathe in those droplets and if they have Coronavirus particles, you can in effect actually breathe those in and contract the virus. The thing you want to understand with the N95

respirators is there's a little bit of a regulatory requirement that we need to understand and go through. So I'll roll into that with the next slide here. So with a lot of the mask mandates that, whether you're looking at it from a general contractor that you might be working for, whether your own company has put out mass mandates for your construction projects, or just looking at it from a state and local government perspective, there's some differences in terms of how OSHA is approaching what a mask is and how they're approaching what an actual respirator is.

So in terms of the regulatory compliance with things, if we're looking at any cloth based coverings, we're looking at surgical mask and things, those are not covered by OSHA whatsoever, okay? The N95 respirators, they are, okay, because the N95 respirators are an article of PPE. So if you put out a mandate that says that all of your individuals who are working on job sites, they need to have a face covering, or they need to have a mask on, okay, that does not mean you are requiring somebody to wear a respirator. So it's a very big difference there. Now let's say for instance, that you get into a situation where you have employees who were doing construction work in a hospital or an area where there's confirmed cases of Coronavirus and for an additional level of protection, you want to tell everybody they need to wear an N95 respirator.

Then at that point, that becomes mandatory usage of respirator. So I've got two things on my slides here. I've got basically charged for voluntary and mandatory use. So essentially the volunteer use that we're looking at, okay, if you just want to wear that as an individual employee, because you sit there and say that I want to provide myself with a little bit higher level of protection, you're not required to be fit tested on that. So there's a fit test that we do essentially, and we do them at SafeX here, and essentially what we do is we set the person who's wearing the mask, and we put them up onto a machine and it measures how well the respirator they're wearing is actually filtering out particles that are in the air, as opposed to what's inside the respirator. So it determines how effective that thing is actually fitting on you.

So if you're just voluntarily wearing a respirator, you do not need to be fit tested. However, you do need to sign what's referred to as Appendix D of OSHA's respiratory protection standard and in the regulatory world, and you look at the OSHA standards and things, that would be 1910.134. Okay? That's the respiratory protection standard. And essentially what Appendix D is, is it's a set of non mandatory guidelines that is essentially passing on the responsibility to the employee who's voluntarily wearing the respirator. So it's telling you how to properly wear the respirator and it's forcing you to essentially accept liability for how you're using it, how you're wearing it, storing it, cleaning it, things like that. Okay? You can only wear a filtering face piece N95 respirator for voluntary use. During the whole pandemic, I've kind of gotten a kick out of, you know, you go into the grocery store and things, and I go into Giant Eagle, and I've seen people that are working at Giant Eagle, they're wearing the full face respirators.

They've got the cartridges on the sides, they've got the full face shields and things when they're working, technically you are not permitted to wear those for voluntary use. So in that situation, an employee would actually have to be fit tested and medically cleared to wear full face respirator. Okay, so there's a lot of confusion when we look at what types of respirators people are wearing, people are getting respirators and masks confused and things. So it's a big area of confusion in the field when we're looking at what people are wearing on construction sites as well as just in offices and things like that. From a mandatory perspective, if you are requiring people to wear respirators, then that's when you as an employer need to make sure that the employees are fit tested, they're medically cleared and they're trained to wear the respirator.

And then that's when you need to make sure that you have a written respiratory protection program as well. So depending on how you're approaching this really changes up the conversations regarding what you need to do as a business owner. So next slide, please. As far as some administrative and kind of overarching recommendations that I could provide as a safety professional to anybody working in the construction industry or manufacturing for that matter today is that, if you have any potential issue or any thought where you might be dealing with this, the best thing to do is in anything, just develop a plan that makes sure you enforce it. Okay? In the world of safety, we talk about planning, planning, planning all the time and how to do things safely, you have to make sure you're planning your work appropriately. The thing I find in the field that's probably the biggest challenge when it comes to COVID-19 plans that construction companies are putting out and things, is that they're just creating blanket policies.

They're not really adapting for what they're actually doing on site and the work they're actually performing. So with respect to a lot of situations where we have local mandates and state mandates and things for masking things, depending on where you're working at, I recognize all of those things, but I can also say that there's a lot of areas where if you want to get buy in from people, you actually have to really look at what's going to be realistic for construction workers to really comply with on job sites and what they're going to be able to do based on their certain tasks. And I will talk about that when we get onto the next slide here. The thing that I would focus on for a lot of the folks in the audience here, whether you're in accounting, whether you're in your financial department, if you work with estimators and things like that, you need to really tell all the people who are dealing with the budgets, the planning, estimating, things like that, that they need to continue to plan and budget for COVID-19 as we move forward. Have to continue doing that.

When everything first started, and there was a lot of general contractors that were requiring the mask mandates and things, there was two issues at play. Number one, companies did not include having those things in their bids because it wasn't in the contract language. I would highly doubt that before all this stuff started, people in their contracts had anything listing about a pandemic. So what I would encourage people to do is budget to make sure you have all the necessary proper protective equipment, whether it's disinfectants, having hand sanitizers and things like that for people to use on sites, that's really critical. But then if you're a GC and you want to create very clear expectations and policies for what your subcontractors are expected to do, you need to change up your contract language. And Tom was kind of talking in the last segment about different things that you should be including in your scope of work and in your contracts and things.

If you have requirements for your subcontractors to be doing certain things as it pertains to Coronavirus, then you need to absolutely list those and your construction documents and your contractor guidelines, things like that. Okay. Then the last thing I wanted to just mention here is that, the best thing you can do is make sure you know, what you're absolutely going to do when you have a positive case. There's a lot of companies that at this point, they've not gone through it, or they have gone through it. We've helped some companies work through this before already. And it's very challenging. It's very scary for companies when it happens the first time. So knowing what you're going to do beforehand is really critical. Go onto the next slide, please. So I will tell you guys this, from a safety perspective, the best thing that you can do is assess your risk across the board, on all of your job sites. Don't just create a blanket COVID-19 policy and expect it to always be enforced and followed by everybody who's working on site because if you don't adapt to what you're doing and what you're working on, then people aren't going to follow it. Okay?

Different trades, different job sites, different things people are doing, where they're working, are they inside? Are they outside? The tasks they're performing? How many people you're working within an area and things, that all is what we're looking at in terms of risk of transmission of the virus. Okay. So I was on a site one time, this was probably two months ago, where the company has a very hard set policy on employees wearing face coverings or surgical mask when they're on site. Okay? And I walked onto the project and there were six guys who were operating six different pieces of mobile equipment. They're moving dirt. Every single one of them are sitting in the cab of their equipment, and they all are forced to wear masks. And with respect to the mandates that are out and things that are out there, I could probably tell you as a safety professional, there are 0% chance that they are going to transmit the virus onto another person in those scenarios.

Okay? So adapt your policies and assess based on what you're actually doing on site. Okay. If you've got people who are working outside and you've got a concrete crew of 10 to 12 people who are working, they pour concrete, they're finishing the concrete and things like that, and they're working in close proximity to each other and they're breathing on top of each other, then yeah, I would say there's a higher risk there, but if I've got one employee who's in an aerial lift on the outside of the building, I don't think there's any reason for that employee by himself working in an aerial lift to be wearing a mask. Okay. So adopt what you're doing based on what you're actually working on on site and how you're doing it. So that would be my recommendation to all contractors and we're trying to help companies go through that, but it is a challenge and there's a lot of legwork that companies have to go through on the administrative side of things to really create these policies and assess the risk properly. Next slide please.

So I just want to talk about some of the things in my next two slides here. I want to talk about essentially what I am seeing as things on, you know, boots on the ground on job sites, things that contractors are doing that I think have worked fairly well. Some of them are unique, some of them are pretty common things, but these are some actions that you might be able to recommend and take for your own company. So the first thing I would suggest is staggering your start and stop times on jobs. And in the summer, this was very easy because we had a lot of daylight and things like that. But if you get into situations where you have temporary lighting on job sites and things, and you have trades and crews who were working inside, I was on a project this summer where what they did was instead of starting the job at seven 38 o'clock and go until four or five o'clock, they actually started the job at five o'clock in the morning and they went all the way to eight to nine o'clock at night.

And what they did was they just staggered when everybody was starting and stopping. So rather than having 60 people who were working on the project on six different crews and subcontractors for all the different trades, all crossing paths for the duration of the Workday, if you had some electricians and plumbers, they might've only been crossing paths for two hours or so. So you were exponentially decreasing the number of times that you were having different subcontractors and trades crossing paths and working right next to each other and things. So they eliminated a lot of traffic that was on their job site just taking that approach like that. Obviously increasing your hand sanitizers that are onsite, your hand washing stations, things like that. At this point, I think we all know that that's something we should be doing and providing our crews, if you have people who are working in trucks and things, giving them the disinfectant wipes, the hand sanitizers and things like that.

If you're a general contractor, you can go out to any supply company and buy those big industrial size hand wash units. So those are really easy to put on job sites, outside your Porta Johns, things like that. As far as your cleaning and disinfecting of tools, if you have people who are sharing hand tools, power

tools, things like that, I don't sit here and think you need to go out and get everybody their own set of tools as far as hammers and all the hand tools that they're working with. But having a cleaning schedule for them is something you should plan for as far as, like I'll just use this as an example, I'm actually originally from Pennsylvania and they had some pretty strict shutdowns as far as what business were permitted to operate, what businesses weren't.

And construction, unlike in Ohio, they were in Pennsylvania, construction was not deemed essential. So for two months, construction in Pennsylvania was 100% shut down. And there was a whole return to work plan that the governor's office in Pennsylvania had suggested and they put out, and there were some things out there that the contractors and the employers, they would have to provide individual tools for all the employees working and things. And for people who buy that stuff, if you're involved in procurement and things for your own business, it's probably not feasible to go and get a table saw for every single employee that works for you. So I think at that point, you sit there and say, we're going to have a regular cleaning schedule to take a disinfectant wipe and things. Or if we create a bleach water solution and things, which is going to give us some level of a disinfectant, we can clean things regularly. So that's a good thing as well.

Regular cleaning restrooms and things, this probably should have been done more before. I mean, if we look at like the Porta Johns and things like that, I've been in some pretty bad ones on construction sites, as I'm sure most of you folks have, but a lot of companies have started to increase the cleaning schedule of those from once a week to two and three times a week, they're doing more disinfecting, doing more disinfecting of like the door handles, the hand rails, things like that. So next slide.

A recommendation I would have, and I've always had this and this is even pre Coronavirus, okay? And when you look at doing cost benefit analysis and things like that, as far as having your safety equipment, okay, I would really urge you folks to push to your people who were involved in procurement to buy individual personal protective equipment for your employees.

So if you're looking at things like harnesses, a face shield that people might wear when they're grinding, welding hoods, things like that, things that people are going to be wearing, and it's going to be very close, you know, on their person and things like that. I would say that sharing those things among eight to 10 people on a crew is probably not going to be the most sanitary thing, because I could assure you that they're not going to be disinfected and sanitized between people using them and things. And the other thing as well, if you actually buy people their own equipment, you're going to learn something pretty amazing, that stuff's going to last a really long time, because when you start having people with their own equipment and buying, and they have their own tools and their own harnesses and things like that to wear, they're going to take a lot of pride in it, they're going to enjoy having their own stuff, and they're going to make sure it's stored properly, it's used properly and they're not going to damage it. So there is, from an investment standpoint, I think you're going to see a lot of return on investment. You probably end up spending less money actually, by buying people their own individual forms of PPE.

Next thing, and I know in construction, not everybody who's actually working out in the field, they're as versed in things from a technology standpoint, this was a big challenge for a lot of people, but it's probably a good idea for the duration of this pandemic. If we could do some virtual project meetings, scheduling meetings and things like that, we have that capability now. So the final thing I'll mention here is ultimately if you have people who are congregating and things like out on break times, lunch times and things, just ask people to try to spread out during lunch and if they can eat or take their breaks in their cars and things like that, that'd be another suggested thing as well. Go onto the last slide here.

So I think the last thing I want to talk about and touch on here is, what are you actually going to do when you have a positive case? And at SafeX, we have helped businesses through this. We have been on sites where we have been around people who have tested positive. We have had people who were working on construction projects and in manufacturing facilities all the time. So the thing I think you have to understand and recognize number one first and foremost is if you have a positive case, should probably at some point be expected and you just have to really remain calm. If you've discussed and talked about this beforehand, and you had a plan for it, then you should be pretty well prepared. I think the first thing you should be doing is working with your attorneys to craft a letter, the sit there and say to inform people who need to know that there has been a positive case at your facility on your job site, however you approach it that way. Okay?

And then as you kind of slide down there and going through this flow chart, it's interesting because especially when you look at construction companies, a lot of crews are pretty small and things like that at times, everybody knows who the person was that may have tested positive, but you can't tell anybody who the person was who tested positive. Okay? You can identify the individuals you need to quarantine and things like that, but you are not permitted based on HIPAA laws, privacy laws, things like that, you cannot tell anybody who that person was.

Something that might be a little bit of a surprise to people is that actually, you are not required to do the contact tracing as an employer. That's actually all done by local health departments. It's done by state health departments and things like that. So when somebody tests positive, those individuals will contact the individual who's tested positive and they go through the contact tracing where they've been, things like that. And then they notify the people who need to be quarantined, whether it's a 10 or 14 day period at that point. At that point following, it's up to the employer to determine what necessary and additional steps you want to take. So if you have, let's say that there's only two people that local authorities say need to be quarantined on a crew, but you want to quarantine all six or seven people just to be cautious, you can do that. If you want to do a deep clean of the project, if you want to shut the job down and things, you can absolutely do that as well.

It's all up to you as far as what you would like to do as an employer and as a business owner at that point. Ultimately, the last thing I will note here is that it is probably a recommended good idea to at least informally do some level of contact tracing at your company and things, and part of that is because if you can prove that there has been an exposure that has happened at work, then that illness can become an OSHA recordable injury. So if you deal with any of the record keeping things on your end of the business, understanding that COVID-19 does have some level of OSHA record keeping component to it. So that's all I had. We'll go onto the next slide. I'll be happy to address any questions if anybody has anything.

Doug:

Thanks, Travis. That was great information, the experience that you've got obviously dealing with this is tremendous. So certainly I would always reach out to the folks at SafeX if you have any questions along those lines. As we wrap up here, certainly want to thank all the panelists, but before we do, Shawn, there was one question that came up related to your presentation, had to do with security operations centers. Can you touch on that briefly?

Shawn:

Yeah, sure. So as threats evolve, there are companies out there that have stood up security operation centers to basically monitor, we talked about monitoring earlier, right? So what that organization is trying to do is provide 24 by seven or eight by five monitoring within your environment. That's the direction we're going, frankly, all the way down to the small business, cyber has those capabilities. I would encourage our attendees to, again, start with an assessment, start with a risk assessment and overview of what controls you have in place first. And then we can guide you in the direction of having a security operation center or what we would call a managed security service. Our service is managed security and information technology services division of Rea & Associates and I run that, but again, it's a great question and everybody, all the way down to the small business, is going to have to eventually get there.

Hopefully that's helpful.

Doug:

Thanks, Shawn. Appreciate you getting back to that question. And again, wanted to thank all the panelists for their time today. Particularly our external guests, Joe Urquhart from Overmyer Hall, Tom Nocar from Porter Wright, and Travis Spagnolo from SafeX, as well as my colleagues here at Rea & Associates, Joe Popp, and Sarah Sparks from the state and local tax area. Shawn, obviously from Cyber and Scott Bechtel and myself from our construction group. So on behalf of everybody, thanks for tuning in today, we will make the slides available. I believe also there will be a recording available, although obviously cannot get CPE credit since he did not do that live, but all of the individuals you see here are certainly available for questions offline as well. And we thank everybody for attending, and we'll look forward to speaking with you again soon.