REGIONS BUSINESS RADIO - Ransomware

Speaker1: [00:00:09] It's time for a special episode of Regions Business Radio. Now here's your host, JD Mealor.

Speaker2: [00:00:20] Welcome to Regions Business Radio. I'm your host, JD Miller, and we are doing a series of episodes on fraud. Business fraud, check fraud, ransomware, business email compromise, all fraud topics that you, as a business owner or executive should be aware of. And I got to tell you, he's not a former fraudster, he does help the bank protect you, protect our assets, protect our clients and our customers. In regards to a variety of fraud vectors, which is a cool term that I've learned from my friend Jeff Taylor. Jeff, thank you for being with us today.

Speaker3: [00:01:00] Thanks, JD. It's an honor to be here again. I'm just so grateful for the opportunity.

Speaker2: [00:01:04] It's an opportunity that we need to take advantage of because our clients, our customers are facing the bad guys every day and they're not even aware of it. And our topic today, I think is very interesting. It's one that's both frightening, it's complicated, and it's beyond impactful if you're a victim of ransomware. Right, Jeff, what is ransomware?

Speaker3: [00:01:33] So let me start JD by saying my background is in payments. So I'm not a cybersecurity expert. I'm not technical in that respect. But I have learned so much about this attack vector. And it is so, so impactful to companies. And we continue to see more and more instances and reports of ransomware. As a matter of fact, one of the companies that tracks this information says that ransomware increased worldwide 70% in 2023, so almost double what they had anticipated or what they had experienced and reported in years past.

Speaker2: [00:02:13] 70% increase in ransomware incidents. Incidences around the globe correct your background in payments. Your experience on the bank side can certainly help customers combat these types of things. And I wonder if our listeners, they may have heard the terms ransomware, maybe you maybe you've heard about it

on another podcast or a TV show. I've seen clients fall victim unknowingly to ransomware and it is frightening.

Speaker3: [00:02:45] So typically the definition for ransomware lies in how is the information, how did the penetration occur and how is the information going to be used. So often we confuse ransomware with malware. We think about the introduction of malicious software into the network of the victim. Well, in a ransomware environment, there are purposes behind that introduction okay. So they're typically to acquire a ransom. So what they would do is they would the fraudster would penetrate the network, enable this malware, this malicious software within the network that allows them to get to sensitive files, and then they contact the client or the victim and demand a ransom payment to get the information back. And think about it, you're dealing with criminals here, so you're not going to get the information back you are paying them for typically the encryption key or the ability to unlock your network and remove that malware from your network.

Speaker2: [00:03:53] All you got to do is power down and restart.

Speaker3: [00:03:55] It'll go away. No, it doesn't work like that. They know they these things. If you think about the old remember malware used to be called, we called it a Trojan horse or we called it Trojan malware. Well that goes back to the Greeks who created the Trojan horse and were able to penetrate the wall of the city by having individuals hide inside of that horse. Yeah. So what happens in a in malware typically is that the software is malicious in a way that's very difficult to detect. And so the fraudster is able to worm their way into the network, get access to those sensitive files and then capture that information for further use. It typically occurs with something like clicking on a malicious link on a website. Uh, it could be the downloading of a file that was emailed to an individual, or it could even be something as simple as code that is embedded into a USB drive, a jump drive that's left in the parking lot, and that jump drive may have something on there, like W-2 files or employee bonuses. And so a curious individual picks up that jump drive, plugs it into their laptop or their computer inside the office behind the firewall because they've already logged in because they're curious about seeing whatever information might be on there, and then it ends up infecting their machine.

Speaker2: [00:05:34] Wow. I could ask probably a thousand questions just from what you just said. And as you're saying that I'm thinking about a client of ours that was victim of ransomware and they never really were able to figure out how the fraudster got in. Right. A variety of things. I mean, simple steps. Don't click on something from a from an untrusted source. Right. We're trained at the bank to make sure that you're viewing the email if something looks off. I mean, it's to the point. Now, I don't read a lot of emails. Don't tell anybody. How is someone targeted for this, Jeff? I mean, how do the criminals target XYZ company or they just shot gunning and trying to get as many as they can?

Speaker3: [00:06:17] Oh no, it's it is. There's method behind it. So typically the fraudsters are socially engineering individuals. They know they look at sites like where we may post information about our job description or the things that we try to do and through social media. And they look at that information to determine is this individual, do they have payment capability? Do they have an option to be able to originate a payment or access to information that that I might want to acquire as a fraudster, or are they just appearing to be vulnerable in some way? And so once they have that information, they began targeting specific individuals. Now some of this is random. JD, I mean, they acquire email addresses off of the dark web. And again, we're back to the dark web.

Speaker2: [00:07:09] To the dark web. Yeah.

Speaker3: [00:07:10] They acquire these email addresses and just it's a shotgun approach. And so they know that if they've got 10,000 email addresses, they may get 100 hits or they may get one hit. But whatever it is for them, it's all about what they're going to do with the information when they get it. So oftentimes it's how do I monetize this information? So speaking of.

Speaker2: [00:07:33] Monetizing it on average, what is a ransomware. What's the worm I'm looking for I don't even know what the yeah. What's a ransomware payment a hostage payment or something.

Speaker3: [00:07:42] Well, typically about a million and a half dollars.

Speaker2: [00:07:45] A million and a half dollars. Yeah.

Speaker3: [00:07:47] That's typical. Now obviously there are smaller dollar amounts than that. But it's a million and a half. And you think about the ransom payment itself doesn't touch the recovery cost or the psychological cost for your employees. What you have to do to recover, I mean, I've seen cases where the victim company or organization had to spend tens of millions of dollars to recover and cleanse their systems from any malware and go through the process. If you think about a company that may have 10,000, 20,000 employees, they may have to wipe every, uh, every device in order to make sure that they are starting afresh and starting anew after becoming a victim.

Speaker2: [00:08:36] So let's hit rewind for a second. And somebody uses a, a malware email, and someone in an accounting department clicks on it and unknowingly installs something onto their computer that is behind the firewall that has access to, let's say, an accounting system. Right? What happens? How does that go down? What are some red flags for lack of a better tum? How does it go down? Because maybe someone's heard about it and they know old you know, Bob down the street was a victim of ransomware. But what does it look like? How does it sound? How do you know when it's happening?

Speaker3: [00:09:15] Part of the process, J.D., is has to do with the desired outcome. So what is the fraudster trying to do? So in a lot of these cases, the fraudster is just trying to disrupt a process. Those are literally just disruptors. They're looking at ways to disrupt a process. In some cases it's to stop the flow of information. It may be to stop the flow of, of some critical element. I mean, there's a lot of different things that the fraudster would do from a disruption standpoint.

Speaker2: [00:09:49] Meaning if, you know, if it's extremely severe, then the urgency would be greater and therefore the ransom may be greater. Correct.

Speaker3: [00:09:56] Well, some are just they're not looking necessarily for ransom as much as they're looking to disrupt the process. So they're really in terms of from a financial standpoint, it's more about recovery, the cost of recovery, the cost of the data itself. If it were to be released, I mean, all of that, that kind of. I have seen instances reported of government agencies where the government, their legal process was

disrupted. So communication between like between the jail and the courtroom. And so you've got situations that occur that enable the fraudster to disrupt that whole process.

Speaker2: [00:10:41] Wow.

Speaker3: [00:10:42] But the other the main thing with ransomware, again, is to try to get the ransom. It's try to monetize that information. And so.

Speaker2: [00:10:48] Do they. Can they, can the criminals see into the computer system?

Speaker3: [00:10:53] Oh, sure they can. They know what data they've acquired.

Speaker2: [00:10:56] Are they actively in the system?

Speaker3: [00:10:59] Could be. They could be. And there's all kinds of different things they can do. It depends on how the malware is written, you know, options to redirect emails, to redirect payments, to hide files or take files and move them out of one section of the network into another.

Speaker2: [00:11:18] How is how is it revealed? I mean, I'm a victim of ransomware and I'm working away doing my thing one day at my job, does a screen pop up and say, what about a phone call?

Speaker3: [00:11:31] Sometimes you get the screen pop up, sometimes you notice my system is a lot slower than it once was, bogged down. It's bogged down. It doesn't seem to operate the same way. A lot of companies that have sophisticated network monitoring software may notice a higher degree of activity memory being used and what looks to appear to be dramatic network activity. Okay, but typically, though, J.D., it's not discovered that way. It's discovered when the fraudster contacts the victim in some way, either by the phone or by some other means to tell them, we have acquired your data. We are now owners of your system, and in order for you to get your information back, you're going to have to pay us this ransom. And it's typically in a cryptocurrency.

Speaker2: [00:12:26] I'm pausing for a minute because I'm thinking, you just don't run down to the branch and wire out some crypto, right? That's weird, isn't it? Because wouldn't that wire be trackable?

Speaker3: [00:12:36] Well, if it were a wire, sure, if it were, if but crypto is. Yeah. Yeah, absolutely. I mean, it's much more difficult if not impossible to track because of the way it's going into a more anonymous crypto wallet when that information or those, that bitcoin, or whatever the cryptocurrency is, it's much more difficult to track. Now, federal law enforcement has gotten a lot better at being able to do that. But it's still very difficult.

Speaker2: [00:13:06] So somebody listening is they experience this thing. Maybe their IT guy calls them and says, hey, there's some weird activity here. Our memory is being used. We need to we need to see what's going what's going on. And then the criminal request ransom via bitcoin or crypto or whatever the case is when they make payment, is the situation over?

Speaker3: [00:13:33] Oh no. No, it's and you know, I should mention to federal law enforcement does not encourage the payment of a ransom. So that's a business decision that the business has to make. They do not encourage that. Federal law enforcement doesn't encourage it, because if you think about it, regardless of whether or not you pay the ransom, the fraudster still has your information. They're not giving you back your information. What they're giving you is the key necessary to unlock the malware and be able to then get access back to your network?

Speaker2: [00:14:06] Yeah.

Speaker3: [00:14:07] And they may only they may only capture part of the network. It may not be the entire network, but it would be that that information that's the most sensitive and has the greatest monetary value when they go to try to, to obtain money for that information. So think about it like this JD, you pay the ransom, you get your encryption key back. They still have your information. So the likelihood is the fraudster is going to sell that information on the dark web. And they may sell it in portions. And so they could very well come back to the company a second or third time and demand additional ransom, because they're releasing this information in segments and not

necessarily all at one time. Do. Again, you're dealing with the criminal element. So they're not going to tell you the truth about what they're doing with the information.

Speaker2: [00:14:57] They're not. No. Surely, they're truthful people. They're very, you know, high anyway, who handles the negotiation with the ransomware criminal.

Speaker3: [00:15:08] Typically the company does that, you know, or they'll have their attorney involved. They'll consult with law enforcement. There are companies that actually do that. Do those like.

Speaker2: [00:15:19] An attorney, like there'd be an attorney. There'd be maybe a law enforcement officer, somebody with this experience. Right? Okay, so the ransom has been paid. They still have some data. Or maybe we don't trust them. They still may have access somewhere. Does the client often have to trash their technology and buy new? Is it possible to clean it?

Speaker3: [00:15:44] Oh, yeah, it's possible to remove that. The thing about ransomware and malware in particular is that you really never know to what extent that malware penetrated my network. So it's very difficult to be able to know exactly what happened. There are companies, you know, that's one of the things we suggest immediately. And we'll talk a little bit about this, about engaging your IT vendor to get that IT and vendor or IT partner involved, to be able to look at the network and have those people who are, who are educated at, at those kinds of things to be able to determine what was captured and how deeply did the fraudster penetrate the network?

Speaker2: [00:16:27] Is there, are there, certain industries that are targeted or targeted or business size?

Speaker3: [00:16:33] No, it's across all sizes. I mean, it's just all about the where they think it's more about vulnerability than it is anything else. So it's the fraudster being able to determine that this individual or this company is vulnerable and finding a way to, to get inside. So a lot of this is through phishing. So we talked about that. You know how the email addresses they'll phishing particular individuals. They'll social engineer individuals and they'll get to a place where they realize and find someone who's vulnerable and backdoor their way into the network. Wow.

Speaker2: [00:17:10] I have been in a gentleman's office before where he was a victim of ransomware. Ransomware was installed on his network and he thought he was. Now this touches a little bit on email compromise. I realize what I'm about to say, but this gentleman thought he was emailing me. I'm sitting right across from him and he and he shows me on his computer, sending an email to me, but it never makes it to me, right? It's gone to some fraud fraudster and the fraudster is telling him, well, I need you to do this and take this step. It was almost eerie how well they had it down. It was like, do this now do that and then go here and then do this. And they're sort of calm and collected and they're just in the system and they're going to tell you what to do.

Speaker3: [00:17:58] That could very well be one of the capabilities of the malware that was introduced into the network.

Speaker2: [00:18:03] And I would imagine there's as many malware strains as there are incidences that occur. That's right. They could all look different. Um, we also had a client that was a victim of, of malware, and that company made a decision just to, you know, pay it quickly, get it clean quickly and move on. I don't recall the amount or really the details around it. It was it was pretty much done by the time we were engaged. Don't you think that if you're a victim of malware, whether it's your accounting system, your production system, your HR system, your website, or whatever it is, you probably should call your bank pretty quickly.

Speaker3: [00:18:42] Sure, absolutely. You want to make sure to let your banker know quickly. You know, there are states that have created or introduced legislation that that really will prohibit government agencies from paying the ransom. So what that does is really leads us to what's the most important thing that you can do on a regular basis to, to protect your system. And that's regularly back up your system. So in these cases, with these government agencies and with companies, independent companies, that also is to perform regular backups on your data, if you can do a real time backup where you know you've got information that was processed a minute ago, then then that's the best thing you can do and be able to move that data into either a partition, a partitioned part of your network that requires additional authentication to get to or to even store that information offsite. You remember, in the old days in the banking world had tape drives, big huge rolls of tape, that every afternoon someone had to put those take those tapes

to the vault. And so obviously we don't do it that way anymore. And, and but it is important that you find a way to back up your systems and be able to put that information in a, in a place where it's protected.

Speaker2: [00:20:07] Speak to a moment. I mean, we're not doing a commercial for, you know, the local I.T. companies, but it sounds to me like businesses probably should have some sort of IT consultant or, you know, somebody that that performs some IT functions regardless of size and scope. Because just buying a new computer from some retail company and plugging it into a network, and that vulnerability seems extremely high. And again, in regards to fraud, we're promoting an idea that you've got to think about this differently.

Speaker3: [00:20:45] Yeah, absolutely. You've got to have that awareness and help to educate to your IT department. As an example, the first thing they've got to do is to protect your network. So they've got to build that. What I think about is building this wall that's impenetrable. Yeah. To build a wall around your network that protects that information. So if you think about JD, the number of people working from home now that may very well access the company's network through unsecured Wi-Fi or through a coffee shop or some other way to be able to get to the network where it's not as secure as it would be if we are sitting in our office on that plugged in to.

Speaker2: [00:21:34] Hard wired.

Speaker3: [00:21:34] In, hard wired in. Exactly, exactly. So all of those environments create additional potential vulnerabilities. And so you've got to be thinking about how is my IT partner protecting the network. And then the second part of that is the protocols that they've got in place and the strategies that they've got in place to protect devices. As an example, being not even allowing the use of a jump drive. Yeah.

Speaker2: [00:22:03] We don't I mean, in the financial services industry, we're we do not do that.

Speaker3: [00:22:08] So if you found the jump drive in the parking lot, you wouldn't be able to even plug it into a device and be able to access that information. So those kinds

of rules and those kinds of policies are important that the company establish that information in partnership with their IT.

Speaker2: [00:22:28] So you go back to the cost benefit analysis of this on average for 2022 or 2023, on average, a ransomware event had a bounty of $1.5 million. Yeah, you don't want to wait to pay 1.5. If you could have been paying a vendor, a partner, an employee to maintain a highly secure network. Yeah.

Speaker3: [00:22:52] And so that's really the first thing you think about is, is backups. Make sure I've got adequate backup. The second thing is to you want to unplug the infected device. So if you can narrow down which device actually introduce the malware into the system, you want to unplug that device and you don't want to turn it off because that then limits the forensic capability from an IT standpoint. Okay, so you unplug it. You know, the Cat five cable that's in the back of the hardwire cable that you mentioned, you want to unplug that cable from the device and then disconnect it basically from the network. So you're isolating. Hopefully you may be isolating the malware.

Speaker2: [00:23:35] If you can find that that individual device. That's correct. Can it jump from like a laptop to a to an iPhone?

Speaker3: [00:23:43] You know, that's a good question. I don't I don't know that. I mean, I guess if.

Speaker2: [00:23:46] You use your iPhone to access your network or whatever, it probably could. Yeah.

Speaker3: [00:23:50] Yeah, I would think so. If the if the malware was introduced to the iPhone or to the, to your, your mobile device to begin with, then then yeah, that's very possible.

Speaker2: [00:24:02] You're checking your work email on your iPhone. You download something that could infiltrate your phone. And everybody, people, companies have their accounting software on their phones now. So it's all that is that is so frightening.

Speaker3: [00:24:17] And you think about using your mobile device as a hotspot. You know, if the mobile device is impacted and infected, then you're logging in with a different device, but you're using your mobile, your mobile device, as the hotspot to get to the network.

Speaker2: [00:24:32] Yeah, that is true.

Speaker3: [00:24:33] So I mean, it's extremely, very, very possible.

Speaker2: [00:24:36] Who else should be on your sort of fraud prevention and detection team?

Speaker3: [00:24:41] Well, you know, definitely your IT vendor or IT partner. Yeah. Uh, I think also you need to make sure that you have when, you know, when you have become a victim, reach out to your legal counsel, get them involved, get the executive members of the company involved, your insurance agent. You want to make sure that you reach out to your insurance agent and certainly your bank. You know, many people think that because they have a cybersecurity insurance that they've got coverage. But I can tell you the underwriting standards for cybersecurity insurance are changing dramatically. And so the insurance carriers are looking more and more to the company to be able to have. Proper controls on their side to help limit yeah, these possibilities and limit the vulnerabilities. They want to know what your response plan is going to be. And so they will ask you, tell me about your employee education campaign or your employee education program. Tell me about what you're doing to help prevent phishing or to prevent unwanted email coming into your network that might have those kinds of attachments.

Speaker2: [00:25:53] Well, you know, I love to be a little facetious. Come on, Jeff, I mean, really, I don't want to have to buy this insurance. And, you know, that's an additional expense because I got to pay for this policy. And, you know, do I really need to include that in my contingency plan? Yeah, the answer is yes.

Speaker3: [00:26:11] Yes, absolutely. To your point earlier, you've got to let your banker know what's going on. It's important for us as the bank to know, not that we're going to help you in terms of, of or that we can help you in terms of the technology side.

Right. But what we can do is help then increase our vision toward monitoring of other accounts. Yes, monitoring other information and just getting involved in terms of what else might be compromised in this situation.

Speaker2: [00:26:42] Yeah. Sort of the diligence around it. If we know that you've been a victim of ransomware, then we can monitor the account more closely. Which, by the way, is an individual effort. We don't do that systematically unless there's, you know, new product that that someone like yourself would create and bring to market. But I mean, you know, typically we have someone, a banker of some, some sort monitoring the account, knowing that ransomware has occurred. Do we have any products? Are there products or services outside of a very robust IT vendor that you yourself would choose? Are there bank products to help with ransomware?

Speaker3: [00:27:18] Uh, you know, that's a good question. I'm not aware of any just because of the broad nature of ransomware. I think the thing we try to do, JD, is lean into education and awareness. Being able to have podcasts just like this, videos that we produce, information that we provide to clients on a regular basis to help them create this fraud awareness mindset and be able to think about, oh wow, you know, I'm I may be vulnerable in this area. And, you know, I think it's important that clients have regular vulnerability assessments. So it's this partnership with your IT vendor to say try to hack me, you know, try to get into the network. What where are the gaps in our network that we need to know about, that we need to that we need to make sure that we're protecting ourselves and things about like multi-factor authentication to require additional authentication factors for your employee to be able to access your network.

Speaker2: [00:28:22] But it's so inconvenient, Jeff, I know, but things.

Speaker3: [00:28:24] Like even as simple as your password protection, you know, if you require a four-digit password, then.

Speaker2: [00:28:32] That's so 1990s. I got a four-word passphrase or some something like that. You know that I can never remember.

Speaker3: [00:28:40] Yeah, no, passphrases, is really what's recommended. Now. You know.

Speaker2: [00:28:43] I know some CPA firms that are doing some vulnerability assessments. Right. And I think there are instances in financial audits that require exactly some summary of that.

Speaker3: [00:28:56] And I can tell you your insurance carrier is going to ask for that information. They're going to want to know that.

Speaker2: [00:29:00] And I appreciate you bringing that up earlier because they're going to poke at it too, right. Meaning that they want to know that that that the network is safe. Because as you and I have both experienced recently, the insurance companies, they're going to begin to focus more on customer vulnerability as opposed to now, look, of course they're going to dig into whatever transaction may have occurred. But if I hate to say, if you're asleep at the network, then you know it's likely to happen, but you can't be asleep at the network level.

Speaker3: [00:29:34] No.

Speaker2: [00:29:34] Absolutely not. What did we miss talking about in this this this is we wanted to be very measured with this topic because of the complexity. It's so various that it's hard to be specific, but at the end of the day, we've got to just raise the awareness right. And don't please, if you run a business at any level, work this into your regular quarterly management meetings. Weekly. Monthly. You know, you might say, well, weekly is a little too frequent, JD, but I don't know. The first time you get, you know, you get a ransomware notification daily would almost be, you know, not enough. But we want to raise your awareness. That's the best way, as Jeff mentioned, to combat this. And if somebody is lazy about it, you need to talk. Talk to him about it. You know, have a have a good old corporate coaching session around. Don't allow yourself to become lazy around protecting the network or, you know, certainly I love the point about zip drives or thumb drives or whatever they are. So it's a broad topic. It's very specific. But what else would you say to a business owner and executive in regards to ransomware specifically?

Speaker3: [00:30:49] Well, I think it boils down to your, again, employee education, because if you think about it, our employees are the most vulnerable targets. And so

being able to not only educate at the C-suite level so that the C-suite executives know that this attack vector exists and that there are vulnerabilities there, but it's pushing that information down to the employee level so that employees are aware. It's like it's things like having programs, education programs and educational material that the employee has to go through this process of taking these classes or signing off on, on a document that they have been exposed to say, yes, I have read this, and I am aware that these kinds of risks exist so that they think about it. It's all about when you have this fraud awareness mindset, it's about pausing what you're doing and thinking through this transaction of where am I vulnerable in this?

Speaker2: [00:31:55] But their boss is breathing down their neck. They got to get this thing, whatever this thing is they got. I'm being facetious again, but I'm playing the devil's advocate. I know, but.

Speaker3: [00:32:03] I say this about business email compromise all the time. I would much rather explain why it's taken me a little longer to do something than to explain that I just lost a half $1 million. Oh yeah.

Speaker2: [00:32:14] Well, and even this ransomware thing confessionally I've been thinking about sort of the, the business office or the C-suite, but I also think about manufacturing companies that we know that have, they may have a, let's say it's a big manufacturing system or it's a production line of some sort. And inevitably there's one, two, three computers that are running that thing. Ransomware could even get out there on a production floor, could it not? Absolutely. And somebody may be used to hitting this button and running this tube. Whatever the manufacturing process is, even to that level, you've got to be aware. Right.

Speaker3: [00:32:53] And what if the ransomware disrupts your manufacturing process so that now, yeah, yeah, there's a redirection of that part or a part that's critical to the manufacturing process that doesn't get introduced into the entire stream of, of, of, of manufacturing. And all because of the case, all because of the ransomware.

Speaker2: [00:33:15] So, so to that point is, please don't silo yourself into thinking that ransomware just occurs in the accounting office, the bookkeeping office, the executive suite. It can penetrate throughout the whole company. And there's safety there, safety

issues. I mean, you think about a logistics company, everything that they do, if you go into a logistics company, there's if you go into sort of a pod, they have all these computers and they're negotiating loads and they're figuring out the frightening thing in my mind is if ransomware gets into that situation, the panic that could ensue, you just got to be aware of it. That's right. What would you say? I mean, to anyone that's listening, sort of in closing, and I'm going to share a couple of our resources with the listeners too, but pretend that that I'm an executive of a company in XYZ hometown, wherever you may be listening to, and you have just a few minutes with that person, what would you say to them? Talk to me like I'm the listener. At this point, I.

Speaker3: [00:34:16] Would say, J.D., work closely with your IT vendor. Understand the things that that we've talked about today, that you need to be having that conversation with your with your IT department or your IT vendor to understand how are you protecting. You're my partner. How are you protecting my network? What kinds of protocols do we have in place to help protect the network? Again, simple things like multi-factor authentication, ways that you can protect the communication between the individual, your employee and the individual and the sensitive information that's in your network. The second thing would be, again with the IT vendor. How are you backing up my data? How often are you backing up my data? Where are you backing up my data? Where is it stored? Who's got access to it? How do they get access to it all that kind of thing that when you start going through that checklist, that mental checklist of protecting your assets, how do you do that? And then I just think it's critically important to have that employee education and awareness campaign. You have got to have a program in place. Place where your employees understand that they've got to be careful about what they post on social media. They've got to be cognizant of these kinds of opportunities and attack vectors that fraudsters are using nowadays to try to get into a company's network and get that information that's so critical to running your business. And again, it's not always about the ransom amount. It's about the recovery. And when you think about what's it going to take me to recover my business, recover my reputation, recover the data that has been lost as a result of this, that's preventable.

Speaker2: [00:36:08] Yeah. And to if I were speaking to a business owner and I would say convene the interested parties. Oh, absolutely. Not just the IT team, your insurance person, you know, your executives around and you need to have a plan. Yep. Exactly. If

this if this happens, what do we do the moment after. That's right. And then you've got to follow that plan.

Speaker3: [00:36:30] And I don't see this declining any time soon. You know I think it does take a more sophisticated fraudster in most cases to carry this out. Okay. But I just don't see that it's going to decline any time soon. And do you think the.

Speaker2: [00:36:43] Fraudsters get promoted from check fraud to like, like they get a promotion to the big ransomware team?

Speaker3: [00:36:50] I think it's also important to note, too, that none of the things that we've talked about today will guarantee that you won't become a victim. That's true. So it is true. So there's still always the possibility that's out there. You know, it's a scary situation and we really don't know who is going to be next. But the chances are pretty good that there is some vulnerability there.

Speaker2: [00:37:14] Awareness can help prevent it. But awareness can also diminish the impact of the event. If you make a good point, you know what I'm saying? I mean, so putting you on the spot here, do you know we have a financial education group called Next Step? Do they have a fraud curriculum?

Speaker3: [00:37:31] Yeah, we've actually created some videos and information for that program.

Speaker2: [00:37:37] And I know we're going to talk about some others in a moment, but you said that you can find some of those videos on our YouTube channel. That's correct. And are you teaching those?

Speaker3: [00:37:46] I have been I created some of the content, but they're professionally done very professional videos that are available. They're short. It's 2 to 3 minutes, so it's easy to be able to access that information, download that information off of the YouTube channel and, and put it in the hands of your employees. Well, we haven't.

Speaker2: [00:38:07] Talked about HR and that's something that that your HR partner probably should help the C-suite with. You know, they could create a training program around our regions YouTube channel. And regards to raising the awareness of these topics. Yeah, we have a great desire to educate our clients and even those that don't bank with us around the fraud threats. This is the second of three episodes that we're doing on a variety of fraud vectors. If we don't help you raise the awareness and I would say too, this is very selfish, but of course, your own regions business radio. If your banker isn't talking to you about fraud, please call us. We talk about it frequently. We're very aware of it. Jeff Taylor and I have been on the phone late at night with clients working through these situations. And look, we're not going to say, well, you should have, but we will pick it up and help you from there. I do want to share some additional information. You can find additional resources on our websites at regions.com/stopfraud regions.com/fraudprevention, and doing-more-today.com under the Financial Wellness tab. That would be a great resource for your HR group to look at as well. There's also a government website dedicated to ransomware called Stop-ransomware.gov. Here you can find a number of resources to assist in remediation and developing your response plan. That's right. There you go. That's the resource that we were looking to share. So exactly Jeff, thank you so much for joining us today. Any closing comments?

Speaker3: [00:39:47] No, I think I appreciate the opportunity. Again. Any chance we can get to spread this message is important. So thank you again.

Speaker2: [00:39:54] You're welcome anytime. And thank you for listening to Regions Business Radio.

Speaker1: [00:40:04] Regions Bank member FDIC equal housing lender. This information is general in nature and is not intended to be accounting, legal, tax, investment or financial advice. Regions believes this information to be accurate when recorded, but it cannot ensure that it will remain up to date, consultant, appropriate professional concerning your specific situation. The information should not be construed as a recommendation of a specific course of action for any individual or business. All regions, products and services are subject to qualification requirements, terms, conditions, fees, and credit approval. Regions reminds its customers that they should be vigilant about fraud and security, and that they are responsible for taking action to protect their computer systems. Fraud prevention requires a continuous review of your

policies and practices. As the threat evolves daily, there is no guarantee that all fraudulent transactions will be prevented or that related financial losses will not occur. Visit regions.com backslash stop fraud or speak with your banker for further information on how you can prevent fraud.