Transcript

Joe Galvin: I'm Joe Galvin, Chief Research Officer for Vistage. Cybersecurity remains a key issue, especially in light of the recent invasion by the Russians of Ukraine. We had Mike Foster on a little while ago to share with us some of the insights that he's learned about what people needed to harden their silos. But now, Mike — I appreciate you coming back. Mike's an established speaker, one of the most popular speakers, award-winning speakers. His calendar is full. His presentation on cybersecurity is one of the ones that is most commonly used. Anyway, Mike, thank you for being here. Mike, talk to me now about the risks. Talk to me about what CEOs need to think about with this enhanced cyber threat and the risk they face.

Mike Foster: It is a serious risk, and it's essential to prepare for the solutions is what you want to do. And I wanted to show this slide because there is a Vistage Chair I really admire. He was a naval commander and he told me, "The thing a lot of people don't think about is lowering risk, in addition to preparing a solution." So, we're going to talk about some of them. This is one of the biggest things that your company could face. And it might be your internet, it could be your phone system, it could be your website, but it's something called a DDOS attack. And you may know about these, but just in case you don't, it's when bad actors, they send tons of traffic and fill up the pipe that goes to your website or fill up the pipe that goes to your phone system, or fill up the pipe so your users can no longer send and receive email. Your legitimate customers can no longer view your website.

The attackers use these things called "botnets" that are just distributed around the planet, and they all just send little blips of information to you. Lots of times they're taking over in real-life, unsuspecting companies, so they don't even notice these little bits of information going out. But when you have hundreds or even thousands of computers sending these little streams of information, it overwhelms you. It fills up the pipe you have that goes to the internet, it clogs you up and you can't have that, so watch out.

We've seen a lot of DDoS attacks really kill companies because email's down, your website's down, none of that works. It'd be like if somebody disconnected the internet connection.

So what I want you to do is talk to your cloud provider, talk to your ISP. Ask them, "What do you have in place? What can we do to protect ourselves from a DDOS attack?" Just like in the last presentation I gave, I want to be careful and not get too technical, but when you call your ISP or your IT team calls your ISP, they're going to know about DDOS, and they're going to offer you ways to protect yourself, and they may charge a little extra to do that, but it could be very well worth the investment of what you're going to invest to have that. So that's DDOS.

Something else is to realize — or a huge risk — is orchestrated attacks that are directed at remote workers. We mentioned this last time, a little bit, how the attackers are going after high net worth individuals. But there are companies out there called data aggregation companies that just gather all kinds of information on all of us, including where we went to school, where we drive, what kind of stuff we shop for — everything. So when the attackers get into those databases, they know so much about you and your workers, that they can craft the most believable messages that say, "Click here," or "Open this attachment," or, "Log in," and then they put up a fake login screen, which looks exactly like the real login screens that —

Joe Galvin: Mike, I don't mean to interrupt you, but that happened to us just three weeks ago when we got emails that were copied off of prior emails saying, "Click on this link and enter this special password." Fortunately, our IT team was prepared, we shut it down and all that, but exactly what you described happened to us three weeks ago.

Mike Foster: So that really hits close to home.

Joe Galvin: Yeah.

Mike Foster: And... yikes. Well, thanks for sharing that. And I know it happens. Yeah, the whole fraud thing. There's even initials for it, BEC, business email compromise.

But the attackers have taken this to such a new level, and they know everything about you. So if they say we know about you, they probably do.

Now, if they're threatening to sell all kinds of information, you need to ask them to show you proof that they got it. Anyway, responding to that kind of attack, we could talk about [that] later.

So something else that people don't think of that's important, a risk, you need to make sure you're backing up Office 365, and Azure, and AWS, any of your cloud services because one of the things attackers want to do is delete your ability to restore. I mean, if they're charging you ransom, they don't want you to be able to restore your stuff. So generally they try to get into systems and dwell and look around and try to destroy your ability to restore. And if you think that Microsoft Office 365 is backing everything up, but you're not checking or your IT team hadn't tried to break that and destroy backups, that's something that needs to be tried. I mean, Microsoft offers a way to backup stuff in immutable storage, meaning once you back up your files at that place in Microsoft, they can never be changed, which means you can't edit them, but that's okay. They're backups, right? And it also means the attackers can't do that. Microsoft calls that immutable blob storage of all things. But there are a lot of the backup products you already use in your company that your IT team can set up to back up all of your cloud-stored information, especially Office 365. Be sure that's done.

Something else to mitigate risks: Please measure how long it takes to restore the data. There's something called "return to operations" and "recovery point objectives." I don't want to get into acronyms, but return to operations is what it sounds like. RTO means how quickly do you need to get going again, and the recovery point objective means that they're different goals. For email, how soon do you want email to be running? How soon do you want your ERP to be working? How soon does your website need to be working? So it's a conversation. It's kind of a "tabletop-type" exercise too, initially, that you say, "All right, we're down, we got shut down, this happened. All right, what do we need to focus on first?" And if you've never practiced a restore, it might shock you about how long it takes to perform a restore. So please don't let the first time you practice a restore to be after you break down.

Another risk everyone has got to be concerned about is just simply what if you lose internet connectivity?

What if you're completely unable to get to the internet? What are you going to do? And that's where you want to have other things in place.

Some companies have routers that literally have a 4G modem connected to the router, so if your ISP gets shut down, everything goes through the router. It's going to be slow, but at least your users can send and receive email messages, then that's not shut down. Or some people use ... anyway, they're all kinds of contingency plans I could go into, but you need to be sure that's something you plan for, absolutely, it's what are you going to do if you lose internet connectivity. It's not okay. Got to be prepared.

Also, you need to think about what if your cloud provider has an outage? I mean, that's something out of your control. What if they go down? I mean, there was a little window a while back where Microsoft Outlook Exchange on the web got shut down. Fortunately, it's the middle of the night, and a lot of people didn't know it, but it was really a wake-up call to those of us who are aware. It's like, "Oh my gosh, what if the attackers had managed to shut this down for a year?" That would be tragic. But even without email for a day, that would probably be very painful, so make plans. I do run into companies now that they make plans to operate by hand if something bad happens. How are they going to be able to function? Take orders? Process orders? Remember who owes them money? That sort of thing. So all this is part of [the] risk preparedness conversation you want to have.

And then wrapping up, a huge risk is — and I hear this from CEOs all the time. They're like "Mike, we need more people in the IT department." We have one customer in Atlanta, and they will not let their 4 IT people go to lunch in the same car. Now that may seem crazy, but they would be so lost if they didn't have their IT team. They make them go to lunch in separate cars so if there's a horrible car wreck —

hopefully, there never would be — but that's how serious they are about this. And you need to really treat your IT pros well. IT pros right now are totally overwhelmed. I mean, you can imagine all the things that are happening, and there's a shortage everywhere.

Joe Galvin: Also highly in demand, I was going to say. They're also highly in demand.

Mike Foster: They are. Yeah, it's unreal, especially people who are good at security.

Joe Galvin: Absolutely.

Mike Foster: Huge demand. And IT pros often only get noticed when there's something wrong. You know, I always like to point that out because IT pros are underappreciated sometimes. So here's the thing to do.

I want you to support your IT pros. They're up against incredible odds.

I mean, these are state actors that have ... they're teams of hackers trying to get you, it's not just Billy Bob in his basement in [Albania].

Now, this is a big, big deal. Please free 'em up from menial tasks. [There're] so many IT pros that are busy fixing the phones, and ordering batteries, and taking care of the printers.

And the other one is please don't force them to sell you on security. I'll meet IT pros that are behind on everything because their CEO said, "All right, I believe you, we finally need a new firewall, but I want you to go out and get three bids, three estimates, and come in here and convince me which one we need to get." Your IT pros are busy, that should not be their role. I hope you have someone you can rely on and trust to get you the right firewall, so your IT team doesn't have to rely on that. You've got a partner that takes care of you, and we don't sell firewalls by the way, but you need someone who does, and who can take care of you on that.

And then something else I did want to toss in while I have time, if I have time, tell me to be quiet, but it's essential for CEOs to know that regulatory and legal compliance is not the same as being secure. Some companies will say, "Okay, we got DFARS, we got NIST 800, we've got ISO 27,000. We're PCI compliant, we're HIPAA compliant."

They get these compliance things in place, and then they think they're secure. It's not so. You can be compliant and totally insecure.

Compliance more has to do with checking off boxes that you're doing specific things, which is essential. Security, on the other hand, is all about having people try to attack you or making sure that everything is secure and you can be one and not the other. So it's important.

I don't want you to get breached, and then you think, "Well, we were compliant, how did we get breached?"

So just remember, I mentioned this last time, you're a high-net-worth individual, attackers are targeting you. They are targeting you. So you may not have thought of that, you may not have thought you're a big deal, but you are. They know what's on LinkedIn. They know all about you. They are targeting you. So remember that when you're focused on everything. I really appreciate the opportunity to come back and give you more information about protecting yourself from these big cyber threats in this very uncertain time.

Joe Galvin: Mike, thank you so much for your expertise. Thank you for what you do for the Vistage community. We greatly appreciate you sharing your thoughts today on the risk that CEOs face with cyber. Ladies and gentlemen, Mike Foster, CEO of Foster Institute, and a legendary Vistage speaker. I'm Joe Galvin, Chief Research Officer at Vistage, and we'll be continuing this thread on cyber threats as we ride this out. Thank you for your time, have a great day.