Transcript

Joe Galvin: I'm Joe Galvin, Chief Research Officer for Vistage. The economic impact of Russia's invasion of Ukraine has yet to be seen or felt, but the increased threat of a cyberattack has escalated immediately. So while the war seems far away, the threat is not. It's already here. That's why we've invited Vistage speaker Mike Foster to be with us today. Mike, thank you for coming. Mike is CEO of the Foster Institute. He is one of our most popular cyber speakers. He's been a Vistage speaker for a long time. His program, "Stop Today's Hackers-Empowering CEOs to be Cloud & Cybersecurity Savvy," has never been more important than it is today. Mike, Ukraine seems far away, but this war can come to the CEO's doorstep right now as a cyberattack knows no boundaries. Why should CEOs be concerned?

Mike Foster: It's a great question. It's important to bring up what's been going on out in the world and what's important to protect. So for example, CEOs need to be thinking about their websites or web applications. That's when a customer or someone else logs on, puts in a username and password, or anything that actually runs a program. Those are very, very, very high targets because it's something the public can access. They can be hit from anywhere in the world and bad things could happen, either from people who are not authenticated, or even if somebody figures out credentials, some bad actor finds out credentials and logs in as one of your supposed customers, but could wreak havoc once they get in. So that's a key component.

Along with that, it's important to focus on your network, obviously. That's what people normally think of, and you bet. The cloud services, some people don't think about how essential it is to protect the cloud services because we just assume, "Hey, everything's there. Everything's safe. It's in the cloud. No big deal." And then the last one that is essential too, especially now, it seems like cyber attackers have started going after the high net worth individuals.

In fact, there's a chance that they may start targeting individuals more than companies.

A lot of companies are becoming secure, certainly not all of them, but a lot of companies are. And once an attacker gets into an individual's computer, then from there, they can get into a company because, generally, individuals have access to their companies. But Vistage members are very high net worth individuals and they need to be very, very concerned about the attackers getting them. It's been a huge problem in the past and it's only more so now.

Some of the things that I want to point out that are really big deals is that the attackers have had plenty of time to plant back doors inside networks. Everybody remembers the Solar Winds breach. It was discovered on December 8th of last year, or 2020 rather, but the attackers have been in since January of 2019. That's a long time. The FBI calls that "dwell time," how long attackers have been in. The Apache LogJam remote code execution problem, which means attackers can execute code on potentially any computer out there that runs this Log4j code, which is everything. Even the helicopter for the Ingenuity Rover out on Mars; it's running that code. It's not going to get hacked because it's too far away, most likely, but still, that's just ubiquitous. And it's been vulnerable since July of 2014. So attackers could have

been getting in and planting back doors in companies for a very long time. There are a lot of people that suspect that, and the attackers are just waiting to pull the trigger if you will.

The Target breach. A lot of people remember the huge Target breach. They exploited that, the attackers did, between Thanksgiving and New Year's on purpose because they knew that would be the busiest time at Target. No one's really sure how long they've been in the system, just waiting. So that's why this is so important. And if a company thinks, "Oh, we're safe," don't go there. I don't think anyone's reading this or listening or viewing this if they think they're safe. So that's good.

But when we talk about state-sponsored attacks, one of the best ways to protect yourself is called "geo-blocking."

And that means blocking different connections from different places in the world. And 4 of these would immediately come to mind. One is your web application. So that means your web servers, customers that are coming to see you. For example, our blog ... you can only see my blog if you live in places where there are Vistage companies. Any other countries that Vistage hasn't ventured into yet, we block the access to our web servers. I'm not saying you need to do that, but if you only serve customers in these 12 countries or whatever it is, why even let your website be visible from anywhere else? Why expose it? And the answer is there's not a good reason to expose it. Block that thing.

Network firewall. Obviously, that's what people think of. Office 365. Some executives aren't aware that you can configure something called "conditional access by country." That would be something your IT pros would configure. But that's for logins. So if you've set up conditional access by country and all your users only authenticate from Europe and from the United States and Canada and Australia, you just pick where your users might be when they log on and approve those countries. Now, any other country that tries to log on, someone with an address in one of those other countries will get blocked. And that's good. That protects you from some of these foreign bad actors.

Now it is important to point out that the bad actors can do what's called "proxying." They could take over a location, a network that doesn't even know it's been taken over, in the United States and still connect to you. But pretending like they're in the United States because they're proxying through or relaying through that server. So none of this is a guarantee, but it darn sure helps. That's essential to be used.

And email messages. You can do the same with the spam filter, the geofiltering. We certainly do that. I don't need emails except from specific countries where we do business. And anywhere else, I don't need those emails. So I'll block them and I'm going to encourage you to do so too.

You'll notice that all of these things are very much for you to talk to your IT pros about.

And that's why I enjoy being able to present this in this article or audio or webinar, however you're viewing this because I would want you to talk with your IT pros about this. And that's why I put in some content-rich slides that you'll be able to see that will help you go over this with the IT pros. I don't expect you to remember it, but there are some key points I must highlight.

One of those is putting in web content filtering if the user clicks. I mean, everybody's told, "Don't click. Don't open attachments. Don't click on links." You can put in some technical filters to help that. And the thing about — I put some caveats on the slide, because your IT pros will probably bring this up with you, and they should. But you may find that if you set up your users, for example, to only access websites in the United States and Australia and Canada and Europe, you may find that you visit a website, and the website won't work because the company with that website actually uses tools in some other country. IT may be frustrated by this if you tell them to block all the countries. So, you'll notice I put the bullet: Be careful not to overwhelm your IT pros."

With web content filtering, I encourage you to use a different tactic. With the other recommendations, it's generally best just to block the entire planet and then allow specific countries to come in. However, for the web content filtering, so when your users click a link, can they go access that website somewhere else? In this case, lots of times, it's better to block specific countries as opposed to just everyone blocked and allow the ones you want to allow. So that's important, web content filtering.

And another one that's important to visit with your IT pros about — hopefully you're doing this — the two-step log-on. Insurance companies are requiring this now for most policies. Everybody's getting on board with this.

If you're not, you're behind. Get off your dinosaur and grab a spaceship or something.

But you need to be using the two-step authentication, multifactor authentication. There are a lot of different words for it, but it basically means when your users log on, they have to get a text message, or even better, they have to have an app running on their phone or their device. There are other ways to get that second factor, but you need to put that in place. It makes it more difficult, not impossible, but more difficult for an attacker to authenticate to connect your VPN or get into Office 365 or your ERP that's hosted in the cloud or anything else that you're using. That's essential.

So I feel like I'm going fast, but I think that's okay because we have a limited amount of time and you guys are all welcome to reach out to me if you want to. But I just want to keep hitting these high points of what it is you need to look at.

The firewalls. Everybody thinks of firewalls. They think that firewalls sustain your main protection. It's actually fairly easy to bypass a firewall. You'd be shocked [at] how easy it is to bypass a firewall. But some of the things you do need to do is close all the ports. Now, ports. It's like, "What the heck?" What that means is, as your IT pro can explain to you as well, that you could think of computers having 65,000 TV channels that they're able to tune into, and your computer, or your firewall, will open some of those up.

For example, if people visit your website, then they're going to be using channel 80 and channel 443. Channel 25 is important too. 21 for FTP. They're set ports that attackers are going to go in and try to probe and see what they can get into. I want you to close everything. I mean, that's what we help our customers do is to block everything. I've been so busy with that for the past several days, ever since all this crisis started. And it's all we're doing. It's going out to our customers and probing.

And it's shocking what's open. We've got a customer that, for some reason, remote desktop. If you've never heard of that, it's just how customers get in from the — not customers — your users, your workforce comes in from the outside. That should never just be exposed to the public, but it is. And they didn't know it. So we showed them, and we were detecting all these attacks that are already happening. The port should not have been open, but it was. So that's why it's important to talk with your IT pros.

They may find that they need to leave some ports open. I hope not. But if they do, it's best to limit those exposures and say, "Okay, if we need to leave this port open for a connection from our office in Ohio," then don't just have them leave that port open for everyone. Have them only open the port for Ohio. Now they may need to have that publicly accessible but plan it. Okay. So be it. Then it's essential. But otherwise, please have them look and see what they can restrict. The best way to go is just for attackers not to even see your devices. They go to your address and just think you'd turned off all your servers and they can't touch them from that. They're going to have to get in a different way. And, oh gosh, there are so many other ways too, but definitely lock down those ports. It's essential. And I mentioned that example, exposing remote desktop connections as one of our customers had. And they're working on getting that shut down.

So, something else to keep in mind is attackers break features. I want you to never trust the features to protect you.

Don't trust your firewall that it works flawlessly. Don't trust that your antivirus works flawlessly. Don't trust that Microsoft log-ons work flawlessly because the attackers are always finding ways to get past these. I encounter some IT pros, not yours, but I meet some IT pros sometimes that say, "Mike, we don't have to worry about any attacks because we have..." and they list off the eight security controls they have in place, which are all awesome security controls.

But in their mind, they've already decided that the firewall works as advertised. That antivirus works as advertised. What they may not be thinking about is the attackers buy those firewalls too, and the attackers look for ways to break the firewall.

Attackers buy the same antivirus products, and attackers look for ways to break antivirus. I mean, it's a constant cat and mouse game going on. Just don't let anyone get satisfied that yes because this product is supposed to do what it says it'll do, it'll definitely do that. No, the attackers are getting in, breaking everything they can.

You need to stack these cybersecurity controls as much as possible, have things in place.

Yeah, I could go for hours.

I want you to engage your email servers because email servers, there is technology called SPF DKIM and DMARK, the very bottom bullet point there. But those are built-in as technology that's built into the internet. If you want to go to my blog at fosterinstitute.com, there's a button that says blog, or you can go to fosterinstitute.com/blog. You'll see a recent article all about SPF DKIM and DMARK, and it explains in detail. But it's something you've already paid for. It just needs to be enabled. It's a little bit technical, but there are places out there in the world that'll help your IT pros set this up.

I don't want to get too technical here, but it involves your servers to make sure, "All right. Did that email that came to you, did it get altered since it was sent?" And if it's been altered, it blocks it or at least alerts you, "Hey, somebody messed with this email." It also makes sure nobody's spoofing someone else, pretending, fraudulently impersonating someone else. DKIM can stop that. And SPF. It is just designed to keep people from messing around. But it's not turned on by default. So I need your IT team to focus on getting that fired up. It'd be important.

Another thing to think about are just the essentials. And I don't have time to cover these. They're all in my blog many times. But the critical updates, security patches have to be in place. When you listen to the federal government, what they're sending out right now, that's one of the top ones they're talking about. No local admins. That may not make sense to you if you haven't seen one of my presentations. That's okay. Just know that's huge to get fixed if you have any local admins. Antivirus. EDR. Important.

And then application control, we find, is very underutilized. One of the companies we're auditing right now since last year, they implemented application control. So I have new hope. But application control is something very simple.

What you do is you make a list of programs that are okay to run, and then your IT team tells the computers. It's very quick.

They say, "These are the only computers you can run (excuse me) the only programs you can run." And that's all the computers will run. So if an attacker tries to install, were-going-to-hack-you-now.exe and tries to run that program, the program won't work.

And a lot of IT pros think this is very involved to set up, that it's very technical, that it's going to cost them a lot of time. And the reality is it doesn't have to. There are some third-party products right now that make that relatively easy and trouble-free. And it's just really, really powerful. So application control. These are some of the things that are most important to protect yourself.

That finishes up the protection part.

Joe Galvin: And I say a cyberattack will take your business down as sudden as a heart attack. And in spite of everything that has gone on and is going on, there's no greater threat to your business right here, right now than a cyberattack. Mike Foster, ladies and gentlemen, from the Foster Institute, one of our all-star speakers, a true expert on cyber. Mike, thank you for sharing your expertise. I'm sure we'll come back and engage you as the year goes on, and we'll learn more about this. Joe Galvin, Vistage Research. Mike Foster, thank you, sir.

Mike Foster: You're welcome, sir!