Transcript

Joe Galvin: The war in Ukraine continues to rage and evolve on a daily basis. We see the images of war: burned-out tanks, destroyed buildings, refugees seeking safety. While the first signs of increased inflation are already showing up in energy costs, what we don't see are the new battlefields of cyber warfare. The Ukraine battlefield seems a long way away, but the cyberwar is on your doorstep right now, as hackers have radically stepped up cyberattacks targeting you and your business.

That's why we've asked the Vistage Chair, Joe Musella, to join us today to talk about how CEOs need to think right now about this threat. Joe is a former corporate attorney at one of the world's largest law firms and a former FBI special agent, counterterrorism. He's also a former Vistage member when, as a CEO of a successful company that's specialized in providing subject matter experts to the government to support classified projects in data science and cybersecurity, offensive and defensive, and now a Vistage Chair in Fairfax, Virginia.

Joe, thank you so much for being here and making time to share your informed perspectives, both as an expert and as a Vistage Chair, working with CEOs all the time on this cyber threat. So let's set the stage. On the morning of 20 February 24th, immediately after Russia sent troops into the Ukraine, you in your role as Vistage Chair sent an email to your members saying: "Ukraine cyberattacks: What business needs to know." That email discussed what Russia's invasion of Ukraine meant and its cyber capability to our members. I'd like you to discuss that very topic with us in some depth today.

Joe, what do our members need to know right now in light of this heightened threat?

Joe Musella: Joe, I appreciate the opportunity to talk to the members. Cyber, cyber, cyber — it's all we hear right now to the point where it's easy to get cyber fatigue sometimes, like COVID. But I sent that email because I believed it was important for my members and all business leaders at Vistage to be focusing on this. I'd like to talk about, kind of, from my background why I believe that.

When you look at what the invasion of Ukraine means through Russia's lens, and then from the lens of the U.S., it becomes important to understand how that created a different level of cyber threat to the United States. As an FBI agent, the mission historically of the FBI was to basically solve crimes that already occurred, but it changed on 9/11. Our task was to identify and disrupt future incidents from happening.

The mission became to look at — and look at different lenses and perspectives — look at the intel and identify things that may happen and stop them from happening. If you look at the cyber and what's happening with Russia-Ukraine right now, you see that as a very clear picture of what's coming down the pike. When Russia invaded Ukraine, prior to that invasion, Microsoft actually did an article in CNN about how they picked up very sophisticated cyberattacks and intrusions in Ukraine. And they weren't focused just on the government themselves. They were focused on agriculture. They were focused on energy sectors. They were focused on all different commercial sectors, and that was because they wanted to focus on the economic impact within Ukraine.

We've seen Russia do this in the past. For the past 10 years, Russia has developed probably the most sophisticated cyber capability across the globe, even more so than the U.S., mostly because they're willing to state sponsor it. They've been poking and probing networks for years, and they know how to do it, and they're ready to do it.

If you think of historically how governments act, the term was proportional and appropriate responses. You think of the 1980's terrorism attacks against the U.S. by Libya and our response when we sent in and did the strikes in Libya, those were deemed proportional and appropriate. What is Russia going to do as we enable crippling sanctions against their economy? Our sanctions are designed to hurt their economic, and socioeconomic — to force the people to rise up and say, this is wrong. To feel the pain of their actions. Is Russia going to launch a kinetic strike against the United States? You know, some people think maybe. But, realistically, what's the easy button?

And the easy button is to do what they've been doing for the past 10 years. Launch cyberattacks at the U.S. and focus on those areas that are going to hurt us economically.

So again, it gets back to: "Is it the government sites?" Yeah, they'll hit our government sites. "Is it government contractor sites?" Absolutely. But it's the economic ones that are designed to already hurt a bad supply chain as well. So, look at us as Vistage members, business leaders, our websites, our social media sites talk about all the wonderful things our companies do. We focus on, "I do logistics across the United States." "I do manufacturing." "I'm in the agriculture." "I'm in architecture." Those are prime targets for a Russian operative overseas to be focusing on with the mission to hurt the U.S. economy. So we need to be thinking in terms of why it matters in general, but also why it matters more given the recent events.

So, let's fast forward. As a CEO of this offensive and defensive cyber company that helped the government, we were tasked with determining whether or not a new technology can go on a government classified system. And one of the first steps we did is we looked at, "What are the vulnerabilities of how this attaches to the system? What are the vulnerabilities of the IT product itself?" We do a list, and the list would be massive, absolutely massive. Then we'd start working with the government and creditors to kind of put them into buckets.

And the terminologies don't matter, but think of it like:

- **"Category ones."** These are the critical things. These vulnerabilities can't exist if this is going to touch a top-secret network. Get rid of them. Figure out how to get rid of them, or you're not coming on the network.
- **"Category twos."** These are important and they need to be mitigated. So we need to take steps. Even if we can't eliminate them, you need to mitigate how we're going to make sure that they're not an issue.
- Then **"category three"** are: These are important, but we're going to deal with these later on.

As you look at all the different things you should be doing from a cyber perspective, I encourage you to think of it in terms of these buckets because as a CEO of a company, again, it's just so much being thrown at you, and if you look at just the massive list of you're being told to do, it could be overwhelming.

We all have providers that help us, whether they're internal teams or external providers. We should be looking at those providers from an IT perspective, just like we do everything else. Is this the right team or provider to help my company grow?

From an IT perspective: "Is this the right IT provider that can help me identify threats and help mitigate me into the future?"

Not the IT provider that helped me get my licenses in the past, and I like them. We need to be looking at it from a new lens, and if we're not, we're hurting ourselves from a cybersecurity perspective and also from a growth perspective as a CEO leader.

This is where Vistage can really help, right? You look at what the purpose of Vistage is, and you think of what the purpose of this conversation is, bringing us all together. How can Vistage help?

- First, leverage your peer advisory group. This is exactly what you should be talking about in those group meetings.
- Second, talk to your Chairs. They can be helping on one-to-one with specific ideas.
- Vistage is just also putting together this, Vistage [CEO] Pulse, talking about this exact topic. This is why I'm talking right now. This is going on cybersecurity in light of the invasion of Ukraine. Watch the videos.

I've had the privilege to watching one that's going to be posted shortly by Mike [Foster], one of the experts in this field. It's phenomenal, but it's a lot. Use Vistage to help you understand what that means. There's multiple videos coming out. Look at the resources. Joe's going to be pumping out additional literature to help you. This is what you joined Vistage. You don't have to go [at] this alone. Use all the resources to make sure, as a business leader, that you are identifying the threats and handling them appropriately for the benefit of your business.

Joe Galvin: Joe, thank you. That's such timely information. You know, we've been tracking and talking about cyber since we started, since we started Vistage Research in 2016, and we've seen us grow.

Up to 51% have an active plan, but that means 49% do not. For folks that have an active plan, your suggestion is: connect with your provider, harden those defenses, listen to what Foster has to say on a technical level. What about folks who maybe have a lapsed plan or [are] behind, or have chosen to roll the dice and do nothing?

Joe Musella: Again, all Vistage groups are different sizes, right? You have with different sizes come different capabilities. The larger members have the capability of [an] internal team or extra providers where they've had the time and resources to put together a plan. Even then, I recommend that you relook at your plan and make sure it's up to date.

Now, let's look at our smaller to mid-size companies that really don't have much. Where do you go? There are a lot of different sites: CISA, which is the cybersecurity agency, and that's what I sent my members. It was just a bunch of links: "Here's an incident response plan you could use by CISA." There are resources out there. And again, this gets back to, "How best I can leverage Vistage given my size and my capability? If you have nothing, simplest thing is [to] go to CISA. Go to your group and say, "Does somebody have an incident response plan that I could have?" It doesn't have to be 50 pages. It could be a checklist that just says: "If there's a response, I'm going to call this person. I'm going to do this." It could be as short and sweet as you need it to be, but you need to have something. And I finished my email that you referenced when we started with:

You should never be looking for a fire extinguisher during a fire. So have something ready and handy that you can use.

Joe Galvin: We know from our research that 5% of our members stated that they were, they lost data as a result of an attack, and that was pre-Ukraine. As we see the intensification of these efforts and we see not just Russia, but other bad actors reaching out and not trying to capitalize on this vulnerability, how does this end? Where does this, when do we go back to a normal state? Or is there no normal? We're now in a perpetual state of heightened DEFCON One cybersecurity?

Joe Musella: Yeah. So I think in between, right? There is no more "old normal." We're not at DEFCON five perpetually, which is why I'm having this talk, right? Because three weeks ago, we all should have been focusing on cyber. We know that, right? But why we should care a little more? This is what I'm trying to impress upon our members in this conversation, to go look at those further resources. Why you should care a little bit more going forward. Yes, absolutely. It's going to be a higher focus.

Joe Galvin: Well, it's clear the implications of the Ukraine have yet to roll through the economy, through societies, but one thing that's certain is the cyber threat is real and right now, and where it's always been an issue, it's even bigger now. So Joe, thank you so much for your time to come on and share your expertise. For folks watching this, stay tuned because Mike Foster recorded two separate videos that go into depth technically and more on what you should do. And we'll continue to provide resources on this as this threat continues to play out and we get [a] better understanding of what it is.

So, Joe, thank you so much, not just for your experience and being a Vistage Chair, but the insights you share today and for our members: Understand that a cyberattack can take your business down as sudden as a heart attack, and that's why it's time to act now Like Joe said: "Don't wait for a fire to look for the fire extinguisher." Thanks for your time. Everyone be safe.