Deloitte.

The long-term impact of cyberattacks

Host:

Deborah Golden, principal and Cyber & Strategic Risk leader, Deloitte Risk & Financial Advisory

Guest:

Vanessa Pegueros, chief trust and security officer at OneLogin; board director, Carbon Black

---

Deb Golden:
Welcome to Resilient. My name is Deb Golden, Deloitte cyber and strategic risk leader, stepping in for Mike Kearney on a special episode on cyber. We've now surpassed 20 episodes in the Confronting the COVID-19 Crisis series. And you've heard from Mike. We've been diving into various challenges of a rapidly evolving environment, and the business landscape continues to evolve. That's why this and our regular Resilient series are so important. Today, we're going to talk about the impact of cyberattacks on the people whose job it is to protect the organizations from these ever-present threats. As gaps in the perimeter continue to expand in today's virtual environment, this is a very timely and critical topic. How has the pandemic drastically increased the risk of threat actors? What's the impact on cyber professionals? And what potentially are the long-term effects to those people on the front lines helping to serve organizations?

Today, I'm joined by Vanessa Pegueros, chief trust and security officer at OneLogin. She's also an esteemed lecturer and author, and has served on the boards of organizations that have experienced much of what we'll be talking about today. We'll also be talking about the long-term impacts of cyberattacks. Let's hear what Vanessa has to say.

For those of you joining in to listen, I'm Deborah Golden, and I'm pleased to be joined today by Vanessa Pegueros, chief trust and security officer at OneLogin. Super excited to be able to get to know you a little bit, Vanessa, as we share, to your point, not only things that are going on in today's day and age, but also obviously diving deep into some areas around things that I know are important to you. I welcome you again to today's podcast. So, thanks again for joining.

Vanessa Pegueros: Thank you.

Deb Golden: And one thing for people to get to know, I know as you and I have been chatting, I mean, certainly love the aspect around your volunteering across the community. I'm inspired by individuals who give back so much, and I know you're heavily involved in your local school systems, where you're working on things like disaster and crisis management. And so maybe just, if

you could help get the audience to know a little bit more about you, what drives you when you think about why giving back to the community in the way that you have?

Vanessa Pegueros: Yeah, I think, Deb, part of it is just my cultural background being Latina and I've been just growing up in the culture and how important the family is and the community. And I have always felt a sense of both duty and a little bit of obligation, but to really like take all the good things that have happened to me and help others in my community to have more opportunity or a better environment. And so I think for me a part of what really makes me happy is being able to do that and to, you know, there are so many people that have come before us that have given us so much opportunity, and I want to be able to give back and help others to have a better life going forward and more opportunities.

Deb Golden: How do you find the time and energy to really put all of those passions forward, because they all sound equally as important and passionate to you?

Vanessa Pegueros: Time is a challenge. I mean, I wouldn't be human if it wasn't. But I do think that I try and draw correlations to things, like I try and have the type of work I do be somewhat related to the type of volunteer work I do. Being related to who I am as an individual, how can I maximize my impact in this world by mapping it to really who I am and my unique experiences. So, by trying to draw those connections and correlations, I'm able to like really have things overlap a lot. And it turns out a lot of things that I speak about can be used in various forums. Presentations I create can be used in various ways. Even talking about this topic and how dealing with incident response in my job and managing the human response around that. That's tied to the stuff I do in my volunteer work. So, I try and kind of create a common theme across my life as much as possible. And then, there are things that are very different. Like I love hiking. I love obviously spending time watching my kids, my son play baseball and I have two sons. And I think it is working it all together and it's challenging. And someone told me once you have a list of yeses and nos in your life and you gotta sometimes look at that list and say, am I saying yes to things I probably should say no to? And am I saying no to things that I probably should say yes to? So, I'm constantly relooking, and sometimes I drop things off my list to make room for stuff that's more important to me.

Deb Golden: Oh, I'm liking the list of yeses and nos and the need to constantly reevaluate them. Cause I think just whether it be personally or professionally, things obviously are constantly changing. So, the need to kind of reevaluate is obviously important. And I also know that you're a self-proclaimed education nut. And so maybe you can give a little bit of background on where do you think that stems from? I know you draw a lot of correlations and connections as do I to things that are going on in the world around us. And obviously I think that's part of your creativity process. And so, I'm just curious, were you always an education nut? Did you decided at some point, wow, I just want to dig deep in certain areas, or where do you think that comes from?

Vanessa Pegueros: I think I actually was just wired that way. From a very early age, I just loved learning, just consuming information. I remember even at a super young age, like five or six, going into like the grocery stores, remember when they had like magazine racks, and I used to grab the Scientific America and read it. And I had no idea what I was reading, but I just really loved the science, the math, I was drawn to it very early in my life, and I excelled at it. And I think a key to being successful in life is really kind of building on those strengths. I love learning new things. I don't want to be in a static place. I want to constantly learn, and so things are changing so quickly, whether in technology or even in our society. I just love picking stuff up and learning it. And I think security happened to be one of the areas which I've made my career with in the past 17 years. And it's like, I think one of the reasons it's been so interesting to me is it's constantly changing and there's challenges that you just can't solve easily and to this day are huge challenges. So, I'm drawn to the difficult problems. I'm drawn to learning and constant change and not staying in one place. And so, to me, learning happens to be the top strength on my strength finders. That's kind of who I am.

Deb Golden: Well, I love that. And I love the notion of being drawn to constant change. One more question about your background. I know we have a lot of listeners who are always curious how people have made their trajectory throughout their education, but also their professional world. And so, when I think about and look at your background, you have a degree in mechanical engineering and it looks like your first job out of college was, naturally, in engineering. But I understand you went back to get your MBA fairly shortly thereafter. And I'm curious, was it something you learned about yourself on your first job? Was it something maybe you didn't know in college, or were you, to your comment earlier, were you're just looking for more insight, education, and knowledge to help better round out your capabilities in the professional world?

Vanessa Pegueros: I think it was a combination of things. I think, first of all, I would highly suggest that everybody out of undergrad go and work within a company or an industry for a tiny bit before going to grad school, because I think it does just help refine your understanding of what you're really good at, or also what you may be interested in. Cause when I first graduated from undergrad, I was like, I'm going to go back and get my master's in a technical area. And then once I started working, I realized that there was a lot more to the world than just the technology and there was this whole business aspect, and I really just started to have a strong interest and curiosity around all the business stuff, all the stuff I didn't learn about in undergrad. But I also knew I really loved the technology. So, I didn't want to totally get away from technology, but I wanted to grow in a different way. And on top of that, my first boss out of college, he saw something in me around my ability to manage people and some skillsets I had in interacting with technical people. And so, he was a really strong mentor for me and really pushed me into, "You should manage people. You should think about this." And I think he was right. I mean, that happened to be like a very key thing for me. I manage technical people very well, and that's not always an easy thing to do. And so that combination of him seeing that potential in me, my natural curiosity, and realizing that I was a little unbalanced because I was just

too technical and didn't have enough of the nontechnical stuff. So, all of that combined kind of pushed me to pursue my MBA.

Deb Golden: And it's amazing to hear. And I know we always talk about sponsorship and mentorship, but the fact that you had someone, to your point, see that not only in you, but to help steer you in the direction to help you understand kind of why these components would be valuable. And I guess, so one last tidbit on that to maybe any college students who are listening. Any advice in terms of how to find or gain or garner sponsorship and mentorship. I know it's not always very easy, and I believe sometimes people are afraid to ask and to seek that types of guidance. So, I'm curious if you have any recommendations or advice for them?

Vanessa Pegueros: I think just knowing the people around you that you work with, and your mentor could come in many forms. I remember even my first job, one of the admins who had been there for many years, she actually kind of took me under her wing as well and kind of help me understand some of the politics of the organization, as did a couple other women. So, I was super lucky to have these people step out and help me, but I also realized that was actually not a common thing that happened to me in my career. I was lucky to have that early on, but I didn't have it very much going forward after that first job. I struggled with getting the right mentors and sponsors. And the way I did it typically was I found somebody I really felt like I connected with and I liked them. I mean, there was something about them. And so, I reached out to them and developed a relationship by asking them to go have a coffee or tea and just get to know them and help them get to know me. And then I would tell them, this is what I really want to achieve. And can you help me? Asking for help. Simply just asking, and more often than not people rose to the occasion and said, "Sure, I'll definitely help you. How can I help you?" Then that's a little bit of the discovery process, how you actually get help and how they can help you, depends on the person, their position in the organization, all that. But for me, I had to literally just ask people for that help, outside of my first experience out of college, which I was very lucky to have several people come forward.

Deb Golden: And it takes sometimes a lot of courage to do that. So, to your point, maybe a lot of individuals never think to do it or are afraid. So, I definitely encourage people to have that courage because to see, and to hear the type of benefit that you can gain from it I think is truly exceptional.
So why don't we shift a little bit into your professional career today as chief trust and security officer at OneLogin. And obviously you've got an extensive background. I mean, we were talking a little bit about your engineering background, your MBA background, cyber background, mentioned a little bit, obviously, around the cyber landscape not only evolving over time, but I think we will all admit that the digital disruption that's occurred in the last five months has been quite significant. And so maybe you could give us your elevator pitch on where you see cyber heading. And I don't want to even say in the long term, because I think things are going to be so different today as they are in a month as they will be probably in a year. But I think if you think about maybe through this calendar year, what do you think are the priorities that we need to think about as we move beyond recovery phase, if you will, where most organizations are today, as we know, struggling with, is there a get back to work? Is it still a hundred percent remote? Is it some combination therein?

Vanessa Pegueros: Yeah, that's a million, more than a million dollar question. And there's a billion dollar industry around, a multibillion dollar industry around security. But I would say a couple of things about security in general. People will say, will it ever go away? Will we ever need to stop worrying this? In my lifetime, I don't think so. The characteristic of the cybersecurity space is that people are making money. The criminals are making money through ransomware, through theft of data. In any illegal activity where there's a lot of money being made, it's very difficult to stop that. And there's the motivations, a global motivation, by individuals everywhere who are looking at ways to make money. Sometimes to survive. And I think that's something we don't often consider that, we like to say, all cybercriminals are horrible people, but in many cases that might be their only source of employment or making money to support their family. I'm not saying that that okays them breaking the law. I'm not saying that's the way it should be. I often just tell people they're human beings as well that are, in many cases, not all of them, some are absolutely incredibly greedy, but I think that there are a lot who are fairly in that lower part of the supply chain of cybercrime that are just trying to survive. And I think that when you have that dynamic, it's never going to go away. They're always going to be creative ways that these criminals think about subverting the controls or utilizing the new technology, whether it's AI or other to actually make them more successful in their attacks.

I think what we need to do coming out of this, which is not really different than what we should have been doing before we went into it, but we need to consider that our workforces are becoming more mobile, that the types of devices they're working on are different and they could be using their own device, they could be using their work device, that they are working, they're working in a coffee shop, they're working at home. We have a challenge in the cybersecurity space realizing instead of fighting this natural trend of virtual work and work from any device, we have the challenge of how do we secure that reality of how people are working going forward, building the right resiliency and the right security and the flexibility that is needed. And I think that's really the critical thing we have to continue to emphasize, and there are so many challenges related with that. I don't see that as easy. If it were easy, it would be solved already.

I think cybercriminals are also going to take advantage of the latest news. So, in this case, it's COVID. They're going to target more phishing emails that are themed around COVID. They're going to take advantage of the human being more in these crisis situations. That typically happens in any crisis. Whether it's a massive earthquake that happened in a country, and all of a sudden you see a lot of phishing emails

or schemes around relief funds for the earthquake. The same thing is happening with COVID. It's even taking advantage of hospitals and attacking them with ransomware. So, it's like the worst of people comes out during these crises, but also the best of people comes out. And unfortunately, I think that is just, change the theme of the crisis or the disaster and you're going to see cybercriminals trying to take advantage of that.

Deb Golden: Yeah. And I think it also, to your point, gives opportunities for innovation for everyone, not just us when we think about how we solve the cyber problem, but to your point, to the adversaries, when they look to create more cyber problems. And so definitely think the opportunity is there for both sides of the equation. And I think one thing that we tend to overlook, and again, particularly given some of your passion, I'm going to dive a little bit into, is the human element. So obviously, we as cyber professionals aren't robots. We're living, breathing humans, but we do have to be on all the time, ready to guard our own organization, whether it be the perimeters, respond to attacks. I say that criminals can be wrong a thousand times and just be right once. We need to be right a thousand times. And so, when you think about how much we as cyber professionals need to be on, how do you help prepare your team for this? How do you help to look at this from a capacity of, maybe what are leaders missing when they look at the focus, and what do we need to focus on from a people standpoint?

Vanessa Pegueros: As a cybersecurity professional, in some ways we think too much of this as a technical problem, which there are definitely aspects of it that are technical. No doubt about it. There are tools we need, there are controls we need, and they are absolutely necessary. I think we haven't spent enough time in thinking about, as you mentioned, the human element of how we respond as human beings when bad things happen. It doesn't matter what advanced technology sits around us, we as human beings just have that basic way our brain functions, which is when we get into a dangerous situation or a crisis, you have that reptilian part of your brain, the run, hide, and fight component of your brain that kicks in. And it's a very efficient portion of our brain, and it activates almost instantaneously. It's very fast. And it's all geared around us surviving as humans. And I think that the challenge we have in cyber and just getting our teams to understand is that when a bad thing happens, whether it's, so malware got on your computer or ransomware, whether there's an incident that impacts your team, a security incident, that, we have to realize as leaders, that the first response that humans have is a bad thing happened; I feel bad. A bad thing happened; I feel bad. And every human being has a slightly different reaction to that. And if their reaction is too driven by the reptilian brain, they can't actually access those higher functions of their brain, which deals with like communication and how you plan and how you think about things, because you're so stuck in that first level of reaction.

So, what I try and do with teams is, first of all, I talk to them about this, like, look, I know that this, if we have the security incident, we're all going to feel bad about it. What we can't do is let that portion of our brain take over. And you've seen people who do that, where they just completely go crazy. They start yelling at people, it's complete chaos around them because they're reacting in a way that they're just going from that base level of functioning of their brain, they're trying to survive. And so when a leader does that, that's the worst scenario because everybody around you starts to also feel panic, or they feel, they start to contract within themselves because they don't want to do something wrong, and there's just an element of fear that surrounds everything.

So, what I try and do is I talk to teams, number one, about this. Like, this is okay if you feel this way. But I also try and say, look, we have to put systems and automation in place that allow us not to feel that as much. And what do I mean by that? So, we need to automate a lot of our security processes so that the machine is responding and not us as human beings. And when the machine responds, it doesn't have emotion. It doesn't feel, it just does what you tell it to do. And so, to the extent that we could automate more of our processes, we are actually helping our people not be triggered at that base level of reaction. And when they're not triggered at that base level of reaction, they can operate in the space that human beings operate well in, which is communication and planning and driving interacting relationships and thinking, and that's where we complement these machines, we complement the automation. And that's really what I've been pushing a lot in my teams is, let's automate everything we possibly can so that we, as human beings, don't get kind of drawn down into that base level of reaction and we have the energy and the emotion to actually rise above it and think better.

Deb Golden: Rise above and rise together, right? I think to your example of sometimes when people are off in that reactionary mode aren't necessarily have the wherewithal to be able to stop for a moment and realize not only what their behavior is doing to them as well as others around them, but also then what that cascading effect has or doesn't have particularly as leaders. And so how do you take yourself out of that moment in the heat of the moment to make sure that you're providing the right direction and leadership, but also obviously showcasing the calm, to your point, to not only rise above it, but to then rise past it as well. So, I think very, very valid insight when you think about crisis moments and ways to adjust that. And I think it kind of rolls into one of the other questions that I was going to have for you around something that I know both of us are very passionate about, health and wellbeing, and tying that into when there's these stressors going on in the environment.

And so, what are those tips to, how do you maintain, and it's something I continue to work with my teams often of making sure that we do walk away at points in time to make sure that we're refreshed and truly able to deal with the challenges in front of us, cause the challenges aren't going to go away. Right? They're there every day, they're there every second, they're there on the weekends. And so how do you help your, you know, tips and tricks of making sure that you pay attention to the kind of wellbeing, not only of yourself, but of your team members.

Vanessa Pegueros: There's a few ways to

do it. And it's kind of a progressive thing. You just, unfortunately, it's not just like flipping the switch, but it's actually building some good practices and processes in place. Like one of the best things to do to help people across your organization with this is practicing mock incidents or tabletop exercises. Just really taking your team and the extended team through these fictitious kinds of scenarios and walking them through it. It's pretty amazing that, even when you're walking people through a fictitious exercise and if you structure it properly, they actually can feel like a slightly elevated heart rate and they start to experience some of the physical symptoms of a real incident. And the point being is you run through these, I like to do them quarterly with my team, and then that way you get the organization used to, it's like building muscle memory around these kinds of incidents, and it calms people because now they're like, "Oh yeah, we had that situation. Here's how we dealt with it. This is who we go talk to. This is the process we use." It also helps because one of the biggest challenges during these crisis times is communication—communication to your customers, communication to your board, communication to all of the stakeholders that need to know.

And also, you have to really give your team time to recharge. Like I've literally on incidents had to tell people, "Get off the call and go sleep." Because people will stay up, you know, beyond 24 hours. And then once you're sleep deprived, you literally can't think properly anymore. So, I basically have had to tell people, "Get off the call and go sleep. Come back in six hours or whatever". Being a leader in telling people when they need to take a break, because people are so committed and they're so involved in it that they don't take care of themselves, they don't eat right. It's time to like really treat your body the best you possibly can because it's running under a lot of stress. And I just found or just breathing, I've taken team members through, "Okay, everyone, stop. We're going to breathe. We're going to do box breathing. So you inhale for four seconds, hold it for four seconds, exhale for four seconds, hold it for four seconds." And we do like three rounds of that just to get everybody to stop because they get so riled up and like, we just have to breathe and relax. And I think just creating an atmosphere where your team members check in, just caring for each other in that scenario is important.

Deb Golden: When you think about building habits and your notion of muscle memory, it definitely takes time. And also to your point, the support from leaders and those around you, how do you help continue to carry that momentum and that support throughout organizations when it's not a crisis moment, when perhaps it's a regular day and somebody has been sitting at their desk for 10, 12, 13 hours, because cyber is everywhere. It never ends, it never sleeps. But maybe not a crisis, meaning solving the cyber incident of the day. And so how do you help leaders understand that it is a habit and it is long term to not only perhaps build that habit, but also the benefit of it is repeating it every day, right? Not just doing it when your heart rate's spiked once a month or whenever that's occurring from an incident perspective. So, any advice to keeping that fresh and active throughout the days/months?

Vanessa Pegueros: Well, I mean, I think there's an element, too, of continuous learning involved here. So like when you do have an incident, sitting down and really talking about what, what went well, what didn't go well. I think the challenge with that is like, if you think about it, when something bad happens, everybody just doesn't want to talk about it anymore. That's a very natural human response. Well, let's just not talk about that. Like, yeah, let's just move on. We're going to go forward. So, I think making it a continuous process of when you're not in the actual crisis and talking about the things that went well, having a culture where your people aren't blamed, where people are encouraged to learn from what happened. And I think a lot of times I've seen people feel like "I'm going to get in trouble." They feel they might get fired, the fear of getting fired, and that adds to the trauma of the incident they just went through.

So, I think helping, I mean, at all levels of management, helping them understand the realities of what it's like to deal with a crisis. And talking to the board about it as a leader, I've talked to the board and really promoting like a culture of let's not fire these individuals. I mean, what better person to deal with that next incident than the one who just went through it and learned a ton of things, assuming they learned, right? But I think the natural kind of reaction of a lot of organizations, and I understand some reasons why, but they fire the leader right away. Like there's this bad security incident and the first thing to do is they get, they fire the leader. And the ripples of fear that that creates in the organization. I get politically why that needs to happen sometimes, but it's not always the best thing for the organization or the people in the organization. So, I think there's multiple things that you have to do to kind of build this in organizationally, not only into the individual muscle memory of people, but also organizationally, and how the organization deals with incidents and how, to me, it's the fact every organization's going to have an incident, the real criteria is how did you handle that incident and what did you learn from it?

Deb Golden: Yeah. And I think learning and then applying those learnings, as you go forward will obviously be very critical as well. And so, when we think about learnings, obviously not just, we've got the people aspect, which we've been obviously talking about, we've got the change in technology, so let's maybe talk about that for a quick second. When we think about the fact that obviously cyber continues to permeate all aspects of business, whether that's new threats, whether that's the size, whether it's the fact that we've gone complete/mostly virtual, I'm obviously seeing more and more organizations get on the, I would say offensive, but also get on the defensive in terms of how to adopt new technologies to monitor and detect cyber threats. Because if we don't have a risk-based approach to looking at cyber threats, candidly, we'll be looking at everything. And we know we're already in a stretched organization in terms of some of our cyber talent. Some organizations may be losing budgets along the way. And so do you think, what are the pros and cons of leveraging these types of technology to kind of automate some of the

incident detection and remediation so that there might be some relief on the front line for some of the things we've been talking about to also allow them to focus on the highest and most priority items that need to be addressed?

Vanessa Pegueros: Yeah. I don't know how a modern security team operates without these tools. They're so critical. I know this sounds a little bit broad, but you need to have machines battling machines, so you need to have software battling software. So, a human being can't battle software. I mean, our brain doesn't operate fast enough. To me, one of the more critical elements of software that needs to be in place for security incident response is the software that sits on the laptops or desktops your users are using, because that's where a lot of the threats come in, in terms of phishing, or maybe the user went to a site, they got infected with some malware. The end point, the laptop is, especially in today's environment, they're not working behind firewalls, they're working at home. They're going through VPN maybe, but they're not actually in the office. So, having a very thorough inventory of that endpoint, but also putting the right security software on the endpoint and managing that endpoint actively, pulling those logs from the endpoint into a centralized location where you can correlate and respond in an automated way. Those are all critical elements to today's environment from a technology standpoint. Blocking them from going to sites that maybe they shouldn't be going to. There's a lot of people at home right now, and they could be going to sites that maybe they're not even aware of that have malware on them. And they think it's a perfectly good site, but they don't have the understanding, and before you know it, their system's infected.

So, the endpoint is super critical. There's other tools, like I mentioned, you have to correlate, bring all these logs together. I'm a big believer in SOAR platforms: security, orchestration, automation, and response platforms. Those are important to automate, again, as much as you possibly can. There's tools to, once a machine actually is infected, they get automatically isolated and kind of taken offline of your network until the issue's resolved. So, that's all stuff that five, six years ago was done in a manual way and pretty ineffective way. And today we have the technology to automate a lot more of that.

Deb Golden: No, and I think that you're a hundred percent, right. And I love the analogy and was taking some notes here around machines fighting machines. Cause, again, even as we were saying earlier, adversaries are learning too, and probably at a quicker pace than we are. And so, the need to be able to tackle them together is going to be critical when we think about not only how we're advancing cyber, but also how we're managing and monitoring it. And again, I think if the offshoot of that is the ability to help provide some relief to the individuals fighting the cyber battles every day, it's going to be much needed. Otherwise, we're never going to be able to catch up with the world that we're working within today. Particularly when you think about COVID, it's obviously drastically changed the perimeter of any one organization, let alone the types of workers, remote workers versus in person work, third-party contractors, supply chains, it's all obviously changed.

And again, I look at that as an opportunity, both for us from an innovation perspective and as we think about the cyberattacks. It's unprecedented when we think about that. And you mentioned a couple of types of ransomware and other types of compromises. Do you foresee them continuing at this pace? I mean, meaning exponentially continuing to grow because the landscape has grown as much? Or at some point do you think we're going to be able to kind of tackle the amount of adversaries that are out there and, again, maybe it's a never ending battle?

Vanessa Pegueros: Right now, I feel like it's a never ending battle, but I say I am very fascinated by ransomware because it takes advantage of that human weakness of that kind of reptilian response. Ransomware leverages the psychology of the individual by doing a couple of things. The fear of losing your information on your laptop or your computer. In some cases, that information could be very dear to you, like your photos and maybe you didn't back them up, and you have all these things that mean something. And there's an emotional component to it. Maybe it's a project that you just finished and you put tons of work in. The ransomware like traps the individual. It traps them and says, unless you pay me, and obviously there's a cybercriminal behind the ransomware, but unless you pay me, I'm going to destroy this. And that creates that emotional reaction in a human being. And for that reason, ransomware is incredibly effective. And taken to that next level, you have organizations who have not developed good backup strategies for critical data. So, when they get compromised by ransomware, they have no other choice, but to pay the ransom. So, when you're paying ransom, the criminals have now figured out, like, boy, I can make a lot of money off this. And ransomware is probably one of the fastest growing sources of money for cybercriminals. I don't have the exact stats, but I know it is not slowing down.

And the ransomware is becoming more sophisticated. And there's even ransomware that sets up a little clock and every minute or every, whatever, second or minute you don't pay the ransomware, it starts alerting you that your data's going to be deleted. And think about how that impacts the human response. You're seeing something visually on your computer, that's like, I'm going to blow your computer up in five seconds, in four seconds. It's so ingenious in the way that it takes advantage of the natural human response. And so, I think it's horrible. I think we do need to continue to battle it. I think it's a form of malware that is not going to go away because there is a lot of money being made on it right now.

Deb Golden: I'm equally actually fascinated by it because it plays on human emotion basically, and human response. How do you help articulate and educate these types of concerns when you think about what the boards need to know in terms of cyber and their cyber hygiene or cyber wealth, if you will, as it relates to their position in the market?

Vanessa Pegueros: So, a board should

not dip down into the operational aspects of an organization. I mean, that's really not their mandate. Depending on the size of the organization, though, with smaller companies, boards tend to get a little bit more into the operations. Public companies, I don't see that as much. But it's a balance because you can't sit there and talk to the board about 50 cross-site scripting vulnerabilities and some special APT ransomware. They're going look at you, like, what are you talking about. That's the challenge, the complexity of cybersecurity and trying to explain that to a board. And it has nothing to do with their intelligence. It's a skillset. People have been in this profession for years and years and years. Nobody would look to a surgeon and question, "Hey, I could do that. I can learn to be a surgeon in, like, a year." No, it's taken years and years for this surgeon to develop this skillset. And it's the same thing with cybersecurity professionals. There's so much detailed technical aspects of it that you just can't teach someone that easily.

So, I'm a big believer in, let's talk about the risks. You talk about the big risks, the risks as they relate to the business and what are the bad things. And I try and present five to seven risks to a board, and then help them understand what bad could happen as a result of those risks. And then what are we doing to resolve them? And then continuing to report back on those risks and how, is the risk getting better? Is it getting worse? What do we do? I think the challenge is that, and being on boards myself, the challenge is boards, they feel very nervous about this topic because it is complex and they don't really understand it. But I also say, that's where there's a series of questions to ask, whether it's the CISO or the CIO who's presenting, that will give you a better sense of, do they have a handle on this?

It's not so much that you have to make sure that they're doing—the solution is right—because that's not really the role of a board. It's more, do the leaders have a handle on this and are they putting the appropriate focus and priority on it. That's the assurance that a board needs to have. And then more and more boards are bringing on people with cyber expertise like myself, because they're seeing, we do need someone on the board who has a little bit more depth. So, it's a new, it's a space that's not going to go away. It's no different than making your board a little bit more tech savvy, understanding cloud technologies. These are all the things that are new that these organizations are going to have to make decisions on in the future. So, it would make sense that you up-level the skills of your board as well, to help with those strategic, or help them in their strategic guidance and understanding.

Deb Golden: So, yeah, and I'm sure that's helped a lot of our listeners. We often talk about boards and what boards are expecting and what to do and how to best position. And so, I'm sure that will resonate in terms of, I liked the upskilling the knowledge, but also putting it in terms that are relevant to them and not certainly in the weeds of the operations, to your point. So, let's shift a little bit now to what I like to call my favorite part. Not that I haven't enjoyed the rest of it, but it's rapid fire. And I don't know why I seem to like this, because it's not about the fact that we get to go fast in questions. It's just random questions that I take note on my Post-it as we've been talking to get your insight into a variety of different items. So if you're game. Don't feel compelled; it's not a one word answer, it could be sentences or paragraphs. But it's just kind of a little bit of everything thrown in there together. And so, the first one I'll ask you, I mean, obviously we all lead in different ways and we respond to different situations. We're obviously constantly thinking on our feet as it relates to cyber. And so, what would you, if you had to put a name around it, what does it mean to you to be a resilient leader?

Vanessa Pegueros: I think to be a resilient leader, you have to listen. You have to be okay with making mistakes. You have to create a culture in your team where they don't have fear to make mistakes as well, or come up with some crazy ideas that nobody thinks will work but might work. And then when you fail you, I feel like as a leader, I own the failure, and it's my job to work with the team to make them better the next time. And so not blaming others, but taking that accountability on yourself. And I think being resilient, we didn't talk about this much, but being resilient also draws on your personal ability to deal with tough situations and challenges. And everybody has a slightly different ability in that space. So, for me, I'm lucky to draw on a lot of tough things that I've faced in my life, and it's made me a more resilient leader.

Deb Golden: I definitely think there's a lot to be said for our own personal experiences and how they shape us as we think about going forward. I don't know that we always know them as strengths in the moment, but the way that the evolve us as leaders, as humans, is certainly impactful. And so, with that, how would you describe your leadership style?

Vanessa Pegueros: My role is to put the right team together with the right set of diverse skill sets, the right set of diverse perspectives, to provide some clear goals on where we need to go, to get to know my team members as human beings and what motivates them and what makes them happy. And then to provide the resources to them, to achieve—whether that's training, whether that's money to buy tools—provide those resources for them to go forward and achieve those goals. My job is not to tell them how to get to the goal. My job is to make it possible for them to get to the goal.

Deb Golden: And what are your aspirations?

Vanessa Pegueros: My aspirations have changed a lot over time. I think, I really enjoyed going public with DocuSign. That was like a really fun thing from a career standpoint. I think I've enjoyed more and more working with small companies now, startups. I'm forming kind of that next chapter for myself. I really enjoy teaching and helping people, helping them be successful. So right now, I'd say I've got a lot of puzzle pieces floating around and I'm trying to figure out what does that next picture look like for me? Right now, I think working at OneLogin and helping OneLogin become successful is probably my primary goal. Doing the board work and continuing to open doors for women and people of

color within the boardrooms and then other higher level positions and being a model to, basically, when people look at me as a woman, as a person of color, that they realize, "Wow, this person's sharp, this person knows her stuff. Wow. It changes my model around what a leader should look like. It changes my mind. Maybe I should consider people I haven't in these positions of leadership." And so that's kind of what I'm working on right now.

Deb Golden: And I guess to that same end, obviously as a successful woman with an extensive technical career path, what advice would you give young women, those minorities as well, individuals of color. I mean, regardless when you look at the variety of racial and sexual orientation, that we want to have that diversity in our teams. I mean, I think cyber challenges in and of themselves are so complex, having the more diverse thought at the table is a massive benefit, but I also know that some people may view this as daunting. They may view a technical career path as daunting, perhaps that others don't look or sound like them. What would be your kind of mentorship advice that you would give to someone and the keys to kind of helping them progress in this capacity if it's something of interest? Or even if they have no idea it's something of interest for them.

Vanessa Pegueros: I go back a lot to what are people's strengths. So, knowing your strengths, and I think, unfortunately, especially for girls at a young age, they have aptitudes for math and science, and for whatever reason, I think right around middle school and stuff, they tend to drop off in their interest in that. And, I just would say, don't give up, because society may pressure you, maybe it's not girlish enough to like math and science, or you might intimidate the boys if you know math or science. I mean, I guess, I wish I would just love more girls to follow their passion around math and science. And I think that if you're already in, maybe graduating from college and maybe you don't have a technical degree, but you may still have that passion. I know a lot of people who were math majors who are great security professionals. They don't have any computer science. I think the field of cybersecurity is growing so much, I think there's room for people who have a strong psychology background, who are just curious and they don't mind, you can't be afraid to learn. I mean, you need to develop an expertise, though. And I think that's the thing, it's hard to be a generalist if you want to stand out. So, you really need to pick your thing, whatever that is, and really dive into it and talk about it and write papers and make yourself known in that thing, whatever it is. The good thing about cyber, it's such a broad field. There's areas of compliance and there's areas of law and there's areas of psychology and technology. And like you could take, it has a lot of opportunity, a lot of surface area for you to say, I want to be in cyber and this is the space I really want to focus on, and this is what I want to become known for, and build your personal brand around that.

Deb Golden: And speaking of brand, as we wrap up, and I honestly have loved this conversation so much today, so I appreciate all of your time, but I have one final question when we think about brand and the always elusive, what are the three words that would describe your brand?

Vanessa Pegueros: Let's see. Definitely resilient. Caring in a broad way, caring about the world, the community of everything. And I'd say thoughtful.

Deb Golden: And I would only add authentic because this conversation has been nothing but that. And so, I appreciate all of your insight and all of your great thoughts around when we think about cyber and our people, but let alone also the challenges that we're faced with in the day to day. So again, Vanessa, I want to thank you so much for being with me today. It was a fabulous conversation.

Vanessa Pegueros: Yeah. Thank you, Deb. It was great to talk to you and all the questions made me think as well. I appreciate that.

Deb Golden: Thank you, Vanessa. It was fascinating to be reminded that people are at the center of organizations specifically as we react to COVID-19. It's not just about the technology. I especially enjoyed hearing about your sense of community, your passion for cyber, and how they all come together as we look at facing what's in front of us, not only with COVID-19, but the increase of cyberattacks on our environments. A lot of topics have been covered over the last couple of months, and Mike and I will continue to bring many more. And as the host of our Resilient cyber series, I hope you keep listening as I bring back the insights from cyber leaders across the globe.

If you have any topics that you'd like for us to consider or anyone else that you'd like to talk with or hear from me in terms of these podcasts, please feel free to hit me up on LinkedIn or Twitter. And for more insights across all aspects of COVID-19, just go to deloitte.com and visit our COVID page. You can also listen to the Resilient podcast on pple Podcasts, SoundCloud, Stitcher, Google Play, and even Spotify. And like I said, please feel free to connect with me on Twitter and LinkedIn. Twitter page is go1denhokie, that's G -O- 1 -D- E- N- H- O- K -I- E. Until next time, stay safe and remain resilient.