Bill Murphy: 00:01

Hello, and you are listening to Bill Murphy's RedZone podcast. I interview leaders who inspire me in the areas of exponential technologies, business innovation, entrepreneurship, thought leadership, enterprise IT security, neuroscience, philosophy, personal development, and more. Welcome to the show.

Bill Murphy: 00:38

Welcome back to the show, everyone. This is Bill Murphy, your host of the RedZone podcast. Today my guest is Masha Sedova. She's the co-founder of Elevate Security, which is delivering the first people centric security platform that leverages behavioral science to transform employees into security super humans. I met Masha and saw her speak at the RSA conference in 2020. Her company was in the 10 finalists in the innovation sandbox at RSA.

Bill Murphy: 01:07

It's a really fascinating approach to security that I want you to learn about, because behavioral science, 90% of breaches are caused by human mistakes. And often said that if we can address the human part of security, that we can boost our security programs exponentially, not just by two, three, five percent, but exponentially. Because if we have a staff of 14, two dedicated security and the rest doing IT ops, well if we can get the security team to get hundreds of people supporting our efforts not just with simple little KnowBe4 training, but I'm talking real behavioral science based training, that's very, very functional for a business.

Bill Murphy: 01:57

As you listen to this, think about it from a strategy perspective, your security strategy of culture. Now, I'm sort of the camp of fear like, "If you do this, you're going to be fired." That's sort of my approach. However, what we're really underestimating is the power of positive security reinforcement, and that's what Elevate really brings here, which is their platform uses employee risk. It shows actionable trends and practical feedback to motivate, reward, and reinforce smart security behaviors of employees.

Bill Murphy: 02:28

Just even thinking about sports teams and such, the more you yell and cajole a player on a team, some of the high performers are going to rise to the challenge, but the vast majority of a team is going to become deflated. And so as we get the encouragement parts of our brain online, even just from a neuroscience perspective, their tool set, what it does is it builds up a gamification. It uses behavioral science to motivate. It creates social proof around people that are doing things in a security acceptable way using gamification and celebrity proofing. It also breaks the organization into heroes, champions, and risk takers and segments the organization, what she calls cohorts.

Bill Murphy: 03:15

So, as you look at this approach, I want you to pay attention to it and think that maybe this is something that is an approach that you can take within your own organization as you figure out what type of a security culture you're going to have moving forward. People are going to come back to work soon, and then you're going to have this workforce now that has the ability to be 100% unplugged and at their home, and then 100% back at work again. So what's our security culture going to be like? What's our security strategy going to be like?

Bill Murphy: 03:44

These are concepts I want you to understand as you listen to this really interesting conversation with Masha Sedova, who's the co-founder of Elevate Security and myself. Have a great day.

Bill Murphy: 03:56

Welcome to the show today.

Masha Sedova: 04:02

Thank you so much, Bill. I'm really glad to be here.

Bill Murphy: 04:05

I'm reaching you in San Francisco, and I'm in the Washington, D.C. area in Maryland. How are things in the west coast right now from what's happening with our current pandemic?

Masha Sedova: 04:20

I imagine it's probably pretty similar in a lot of places in the world and in your town as well as in my town, but aside from the lack of eggs and toilet paper in our grocery stores, it's a lot of time at home with family. A lot of time behind the screen, but I got to tell you, it's been a lot of change. Every day looks totally different from the day before, but I've seen a lot of really interesting things evolve from the space in security, in remote working, and also in just personal connections. It's fascinating to be a part of a really large, unintended global experiment that we're in right now.

Bill Murphy: 05:00

It's a really interesting opportunity to lean into, and I love this because our conversation can give people a chance to get out of the tactical fear part of their brain and really into the strategy of security and take an opportunity while they're doing the dishes or catching up in their garden or doing things that you don't need the extra windshield time. You get all this free time now. Let's learn about how we can position our security moving forward.

Bill Murphy: 5:29

Maybe where we can start is maybe you can tell me a little bit about you're the founder of an organization. Maybe talk a little bit about your founding story and how you got started. There's always a spark that you're like, "You know what? I have to start my own business," and I'd love to hear that story.

Masha Sedova: 05:47

Yeah, it's a story I love telling. I'm the founder of Elevate Security, and the co-founder and I started the company in 2017, January of 2017. We come from the background of being security practitioners. I initially studied security in school and worked for the defense contracting world for many years on the Russian cyber threat.

Masha Sedova: 06:10

In 2012 had the opportunity to start and run a team at Salesforce called the Security Engagement Team. In that space when I started this team, I had the opportunity of addressing human risk for the organization. And when I started that role I was given an animated PowerPoint to roll out to my employees and said, "This is what you have to stand up against advanced cyber threats," which was a terrible joke because I had seen what a Russian state sponsored actor could do. I knew that if the only thing that I gave my employees to defend themselves against such a sophisticated attack was mandatory compliance oriented training, the only thing I would succeed in was making them uncomfortably numb to this conversation without actually giving them the tools or the empowerment to actually defend their data and our organization as a whole.

Masha Sedova: 07:03

I remember taking a huge step back and said, "I don't see any solutions in the market right now that feel like they can adequately address this threat, which is ubiquitous." Human error accounts for something like 90% of all breaches, and it depends on how far back you go. It could even be as high as 100% if you account for things like unpatched servers having humans responsible or insecure code.

Masha Sedova: 07:28

But what I realized is that if we could get people to buy into the concept of security, their performance would be so much more than just if it was a compliance exercise. So that question of what would it look like if people wanted to do security instead of have to took me to the fields of behavioral science and positive incentives and gamification. All three of which are the study of how and why we make decisions as human beings and what drives us and motivates us.

Masha Sedova: 07:58

You may have read some of these books. There's a lot of popular literature around this, but Predictably Irrational and Drive and Thinking Fast and Slow and Nudge actually are all known piece of literature on this. But there's a lot of work done on understanding how we make decisions as human beings, but we've never applied it to security. We've just applied the idea of human beings being programmable, and we just send them training and then they'll do something different. But that hasn't been our reality.

Masha Sedova: 08:29

So, I started applying behavioral science framework to the program at Salesforce and measuring its impact in results to see if this was an effective approach, and it started working. It started working in a really notable and drastic way, and so much so that I had the opportunity to speak at conferences about this and right white papers. It was getting a lot of visibility that other customers, Salesforce customers were calling me and said, "Can you help me with my program?" And it was at that point that I realized that the market needed a different solution and that I had an idea that was worth pursuing. So, decided to start the company, and it's been an amazing and wild ride ever since.

Masha Sedova: 09:09

Today, Elevate Security is building and delivering a platform that collects, highlights, communicates, and influences all types of human risk. Everything from phishing and malware to sensitive data handling and secure coding practices. We look at the program in a much more holistic fashion.

Bill Murphy: 09:30

What's interesting is, Masha, when you think about it, most instant way to get scaling and security is to have an exponential number of human beings that work in the company have a higher degree of awareness, you automatically ... I don't know how you would measure this, but if a CISO walked in on day one, and the program was a lackluster program and maybe people's awareness was at 14.5%, and then you could actually scale that in a short amount of time to 80%, that is a huge impact that supports that security systems, but you could never get that effect from just the security system itself, from the technology.

Masha Sedova: 10:15

Yeah, one of the things that we had discovered while we were working on Salesforce is that despite investing in so much technology as you just mentioned, there's still a human element that was consistently at the root cause of incidents and events. And if we weren't thinking about that problem holistically, so it's the technology, it's the processes, and it's the people, we were still leaving a huge portion of the problem not just unanswered, but we weren't capitalizing on all the resources we had to defend our organization. What I've seen is that best in class organizations that do invest in the human element not only just reduce their user generated incidents and so their overhead of clean up, but they actually empower this whole population to be part of their defense, which is a totally different way of thinking about the human element.

Bill Murphy: 11:09

From the brain science, really, perspective you've taken empowering people versus basically, "Wash your hands before you leave the bathroom." It's sort of like we're sort of ingrained as a culture prior to the pandemic that that was an important behavior, but with the security you're saying that we can empower people and that has an exponential impact within the organization.

Masha Sedova: 11:36

This might be actually a good opportunity just to take a step back and talk about how our approach and what we hear about science is and how it's different from what we've been doing in this space for decades as an industry. What we just talked about, we just mentioned is a concept that we're all familiar with, which is awareness. Which is, "Wash your hands before you leave the bathroom." That's all the science we've had, but how many people knew that but weren't doing it beforehand? Same thing with things like smoking. Millions of people know that smoking kills them. They still do it.

Masha Sedova: 12:05

So, awareness is just one very small sliver of the equation. Why it has only been very limitedly effective is because awareness almost doesn't matter. What matters is the behaviors we do. Do we actually wash our hands? Not are we aware of that washing hands is important, but do we actually do this? Do we actually have unique secure passwords across all of our sites or do we just repeat this as rhetoric that's good to know?

Masha Sedova: 12:35

The reason we do anything as a human being that's different tomorrow than we do today is because of three factors in behavioral science. One, we have the ability to do it. So, the action itself is made either easier or more accessible, and I'll give you an example in a bit. We have the motivation to do it, and something reminds us. There's a trigger. Without the combination of all of those three things at the same time, we're not going to do a behavior.

Masha Sedova: 13:06

The thing about what's happening with coronavirus is all of a sudden our motivation to wash our hands is actually spiked. We're now tied into motivation, but the thing is I could be super motivated to wash my hands, but if the store is out of soap, I can't do it. So, that's back to the ability. You need both. I need soap, which is ability. I need the tools to do the thing, and then I need to care enough to do it. I need to have some type of driver to actually do it. Then I need a reminder like the sign that says please wash your hands. "Oh yeah, you're right." You have to sing Happy Birthday twice or whatever it is. All three things need to exist in order for me to successfully wash my hands, and absence of any one of those three will not let me do the action I want to do at the end.

Bill Murphy: 13:51

I see, okay. Now, you have a very interesting LinkedIn page. I encourage everybody to go to it, because you have a lot of those books you just mentioned on your LinkedIn profile. Several of them I have read, and I love reading. There's a woman. Gosh, she's out of Texas. I forgot. She was on the Tim Ferriss podcast at one point, but she talked about gamification. And I noticed in your presentation, how do you use gamification? I know that's kind of a buzzword. Maybe we can drill into what that means so we can take it out of the world of games into what that actually means for security. I'd love to get your thoughts on that.

Masha Sedova: 14:33

Gamification isn't actually about playing games. It's taking game mechanics and applying them to often business processes or something that you're trying to improve the actions on. The reason why games are successful is because they figured out how to drive the things that are important to us as human beings. Things like feedback and giving us a chance to get to mastery and autonomy, so giving us a choice. Do we want to engage in this activity or not?

Masha Sedova: 15:02

And so we see gamification all around us. We don't think about it like that. Your airline points system is perfect example of gamification. You keep flying on the same airline because it gives you more points to get to different status. That's gamification. Your loyalty at your hotel. Your buy nine, get your tenth free are all examples of gamification to drive a specific behavior. Why gamification is important is back to that model that I was just mentioning about the motivation and ability. Gamification helps amp up our motivation to do something. Gamification gives us feedback, gives us an intrinsic sense of accomplishment. It could be concepts like status, it could be achievement, it could be reward, it could be a leader board. But there are many different types of ways of giving me the motivation to do a behavior, and gamification is just one of many tools that we have in our tool belt to actually drive an increase in motivation, which will then change a behavior.

Masha Sedova: 16:08

How I've seen this play out in this past is we see this all the time, like CTFs and bug bashes for secure coding or parts of an organization. I've seen organizations reward and highlight people who have the best streak of not clicking on phishing links or the people who report most often. We can call those recognition or kudos, but both of those examples really lean into gamification.

Bill Murphy: 16:36

I see in one of the examples you wrote the innovation sandbox in RSA, which was really pretty cool. You had a picture of a behavior map of an organizational dashboard, and I was secretly hoping that you would break it down and do the individual level. Because we talk about motivation. I know you kept it at the department level, but I'm sure you could go down to the human being level, right?

Masha Sedova: 17:00

Yeah, exactly. What you're talking about, what we do is we map what the security actions of what someone does on a network based on a variety of security tooling that most organizations already have in place, and we score every employees' actions. Then we give them an individual comparison about how they're doing, but it's not just saying, "Hey, you're not doing great at phishing." The thing that's most impactful is we compare their performance on specific behavior to how their peers are doing and how their department is doing, and that's a concept called social proof.

Masha Sedova: 17:36

We see it all the time in how many reviews an item gets on Amazon. We're like, "Oh great, it has five stars. I probably should buy this, too." Or when you go to a hotel booking site and it says, "Oh, 11 other people are looking at this room," it makes you feel like everyone else is doing it, I should too. So when you can break down a specific behavior you're looking for, and in our case it's security behaviors that we're looking to drive, and we can show, "Hey historically speaking and looking at your specific individual performance," which is one really important point that I'll come back to, "but based on your performance this is how you compare to your peers." That by itself is deeply motivating and drives a lot of change. Before we ever introduce any concepts like training, people understand, "Oh, this is where the bar is and this is where I am. So I need to change my actions to actually meet the bar."

Bill Murphy: 18:30

That's really interesting. I haven't heard of that concept of social proof in security, but I can see how that would be a very, very powerful motivator just in and of itself that it's public and you're comparing essentially your behavior to someone else. Is there an example that you think is ... I'm sure there's a lot of examples, but is there a couple that are, you think, very unique and create quite a bit, from an 80/20 analysis, the 20% that gets you 80% there?

Masha Sedova: 19:02

Is it an example of social proof that would get you there?

Bill Murphy: 19:05

Yeah. I guess clicking on phishing emails would be one that would be fairly straightforward. I'm just trying to think outside the box from your world what other ones would there be.

Masha Sedova: 19:20

Examples, yeah. Like you said, we do highlight phishing click-throughs, how often you click on a link versus people in your department. We've also done things like malware infection rates. So how many times have I had to block something with endpoint technology on your machine versus anybody else in your department. So, you can see that kind of behavior.

Masha Sedova: 19:43

There's another kind of social proof called celebrity social proof where we highlight someone who you look up to, and we say, "Hey, this person is doing it." So it's not just your peers or an aggregate, but we often highlight that the CEO is using a password manager, and we call it out by name and say, "Hey, did you know the CEO, Jane Smith, is using a password manager? You should too." That's another type of social proof that we've seen be incredibly effective, because a lot of reasons why people don't use password managers is they think it's not secure, it's not effective. But one of the fastest ways instead of trying to convince people of all the logic is saying someone who has resources, time, and education, someone you look up to does this, so it's okay for you to do this as well. You're modeling good behavior.

Masha Sedova: 20:32

We see that all the time when things like a celebrity uses a product and endorses it. Marketing has figured that particular play out a long time ago.

Bill Murphy: 20:42

Yeah, for sure. I find some of the CIOs and CISOs that recently have been saying that if someone violates a policy ... Again, just picking on click-throughs for a moment. If they violate that too many times, it's actually now from a board level that person gets reported. I hadn't heard that until late 2019 I started hearing that more frequently. Clearly the boards are concerned, and literally it's a discipline action. Obviously that's at one end of the scale, and then you have celebrity social proofing. I can see both being massively effective. Is there a science around this of what is actually most impactful from an employee perspective?

Masha Sedova: 21:34

When I think about mitigating risk of specific behavior, let's drill into phishing click-through as you just mentioned. I think about segmenting the organization into a concept that I call cohorts. You have your heroes, your champions, people who are demonstrating really great behaviors. You have people who fall into the majority of the bucket, which is acceptable risk. They're doing it, but they're not doing it so often that they're introducing enormous risk to your organization. It's something that you can manage. And then you have your low cohort who have unacceptable risks. They're doing something often enough or with enough severity, even if it's only one event that is an unacceptable behavior to your organization.

Masha Sedova: 22:30

What you're describing is people are clicking three times in a row would fall into your lower cohort. And why that's important is to break your organization into these three different groups by behavior, because every group needs different type of communication and reinforcement to continue driving that behavior. For your champions, you want them to stay in that and model it for the organization. You need to put them up on a pedestal and give them kudos, and that's where you lean in with leaderboards for example.

Masha Sedova: 22:52

Your middle cohort, concepts like social proof and the nudging that we were talking about and peer comparisons is really good for the middle group, because it helps get them motivated to up their performance a little bit. But overall they're pretty acceptable. It'd be great if they were champions, but not perfect.

Masha Sedova: 23:11

And then your high risk groups, that's where you really need to think about how you're going to escalate that. I highly encourage when I speak with CISOs around dealing with this kind of risk and saying, "Have you done an adequate amount of intervention with this person in order to truly move them to an HR and a firing kind of situation?" I'm not saying that that's not the inappropriate outcome. I definitely do think that there's certain people who have demonstrated an inability to have privileged access to sensitive environments, and those should be revoked.

Masha Sedova: 23:47

But I would encourage potentially having a conversation of understanding why they do it before you move into firing, because if we just said, "Hey, I sent them training three times, and they answered all the quizzes but did it again," it could be that person is at fault, but it could be that your training is bad. It could be that you didn't meet them where they were as a human being. Maybe they don't have enough tools or resources to do the behavior well. Maybe their manager isn't supportive. It's more accurate for things like secure coding like if I don't have enough time to review my code and ship it on time. So that could be a management conversation. And just truly understanding have you tried to resolve your load cohort with as much empathy as possible before moving to firing.

Masha Sedova: 24:43

I have seen people completely change their behaviors when you move out of just giving them more training and actually look at the reasons why they aren't doing that behavior, and hopefully what you will be left with is a very, very small percentage of your organization that you'll have to fire because of that, of non-compliance.

Bill Murphy: 25:04

It is interesting, because I love this concept of cohorts and breaking ... You're not treating your high performers and your heroes and champions the same. You have different communication style with the heroes and champions, acceptable risk folks, and then diving into the high risk behavior folks differently. It's just a different way of communicating. It's similar to raising teenagers. If the kid comes home at the curfew hour and does that repeatedly and it's not breaking through, then you can use the same communication pattern. But the ones that are breaking that pattern, then all of a sudden you got to say my current pattern is not working, clearly.

Masha Sedova: 25:45

Right. I never thought about it, but that's a great analogy. That's a great analogy. A lot of what I talk about, everyone's really skeptical, but if you've ever raised children or tried to train a pet, we're using very similar methodologies. Positive motivation of behaviors you want to see.

Bill Murphy: 26:02

Why kick the dog that's behaving?

Masha Sedova: 26:04

That's exactly it. That's exactly it. If it works for pet training, maybe it'll work for securing our organizations.

Bill Murphy: 26:15

I haven't talked to you about this prior, but I listened to you talk about Fitbit for security behavior. I love that because it has a ring. It's like, "Fitbit. Oh, I know what a Fitbit is." I started talking about throughout 2019 about digital twins, and I love right now we have this human ... we had these Fitbits and these different sensors that we can put on our body that essentially we know that if our heartbeat is at a certain cadence level, if it's at 100 beats a minute versus it's sleeping at 60. But if I'm sleeping at 60 and that's a normal behavior, then all of a sudden if I'm in the middle of the night and my heartbeat spikes to 150, I probably have a problem. There's countless examples where the Fitbit has triggered, "Hey listen, you've got a problem. You need to go to the hospital," because your heart's violating an acceptable behavior pattern.

Bill Murphy: 27:11

That's an interesting concept for me, and I call that a digital twin because you can set up literally normal pattern at 60 beats a minute sleeping versus exceeding that by 20% sets an alarm off. I'd love for you to talk a little bit about that of how either within your product set or how you frame that within the security people you work with.

Masha Sedova: 27:32

That's a great example. I like to think about where we were in our fitness world before concepts like Fitbit. The reason Fitbit works and is as amazing as it is is because it runs on data, and it's data we willingly give for insights back. It's back to is this normal, can you keep my trends going, can you keep me accountable, where am I on the leaderboard, how do I compare to peers. But all of that exists first and foremost on data.

Masha Sedova: 28:04

Same thing happens to us in our advertising and marketing technology. The more our computers know about us and who we are, demographics, what we like, the more specific and targeted the marketing ads can be. Whether or not you like that, that's a different conversation. But in security, especially security where it's in training, we're so far behind in this concept. We have as best practices a one size fits all approach right now where every person in a company gets annual security training, and it doesn't know anything about you. Doesn't have any context as to who you are, what you're good at, what you're bad at, what you know, what you need to know.

Masha Sedova: 28:41

The best we can do is, "Hey, I know you're in finance and you probably process credit cards, so here's some PCI compliance." But we haven't applied these best practices and frameworks that we've clearly done for fitness, for marketing technology, for finance and investment. But we've never done it for security education, and that's one of those things that we're trying to track now and help.

Masha Sedova: 29:05

So what we do is we collect the security actions, as I mentioned earlier, that an employee does on a network. So, do you download malware? Do you browse to websites that are blocked? Are you connecting to data that is sensitive without a VPN? Are you using a password manager regularly? Are your passwords reused across sites or are they unique? Some of these concepts aren't necessarily brand new in security per se. [UAVA 00:29:36] technology has done this, but we've never included employees as part of this conversation. It was always the security team collecting this data and monitoring it for anomalous behavior and say, "Oh, this machine logged in from China even though it's logged in from the United States. We should block this account."

Masha Sedova: 29:54

All of this has been without the involvement of the user, which I think is missing a huge opportunity. Because with your Fitbit example, what happens is if we can show that data back to an employee and say, "Here's where you are. This is where you've been. This is how it compares to your peers," we unlock huge amounts of motivation, intrinsic desire to change a behavior, and also it starts becoming a dialogue where you can say, "This is something that I'm seeing as an unusual trend in your behavior. Either you need to change your behavior or can you let us know that you're doing something that's weird and out of the norm so we can train our own models around that?"

Masha Sedova: 30:39

You start treating an employee as part of the ecosystem, as opposed to a weakness that you're trying to design around. I think as long as we keep the human being out of the equation, we are doing ourselves a disservice because human beings are dynamic and complicated, and we can never predict everything we're going to do. The best thing we can do, I think, is have consent around data collection and transparency around what we're seeing and learning from that data so that not just the security team's learning from it, but each one of us is able to get that feedback and uplevel our own security awareness from it.

Bill Murphy: 31:21

I think the irony of today's day and age is really interesting. I've talked for now a couple of years. One of Red Zone's big ambitions is to create essentially a biological response on the networks. So, create systems that are automated at scale. Just like our human biology doesn't ask for our permission when the body has a cut in its left thumb, but the white blood cells aren't saying, "Do I have permission to go deploy resources?" It just goes and does it. Now, I might cut that thumb very deeply and need to go triage it at the hospital, but that's still the automation of the healing is going on while I'm getting the thumb stitched or broken, et cetera. But it's an ongoing process of health and of triage, and there's automation in it, but there's also the kinetic, "I got to go visit the hospital at times."

Bill Murphy: 32:14

It's interesting I have been talking about that biological response in our digital world, and now we have this pandemic threat. I didn't see that the biological takedown. I thought we were all going to be coming from the digital takedown. But what's interesting is that the practices and the ongoing ... I think security is a verb, not a noun. It's not a destination that you can reach. It's always on process, and so I interpret what you're saying at the human level is literally every person is a biological organism within this digital universe, and we have to build it from the top up, otherwise one little infection like in Wuhan, China takes down the whole world. One little human being action can take down the whole company.

Masha Sedova: 33:01

Yeah, absolutely. But the exact opposite can also happen. One human being can detect and attack and flag it for the rest of the organization as well, especially really sophisticated ones that surpass our technologies.

Bill Murphy: 33:17

I really am impressed by what you've put together at your company, and I want to make sure that we talk about things that are relevant that you're bringing value to CISOs and CIOs. What have I missed asking you that you think would be really useful to talk about relative to the products that you put into networks and the services you provide to the individuals?

Masha Sedova: 33:39

We talked a lot about how we engage with users and behavioral components. We do that in an ongoing email communication, and that's really cool for the employees to engage. But for an executive who needs to communicate risks to an organization, and as you said security is a verb. How do you communicate that you're doing well or poorly, especially as it relates to human risks? This is one of the other really large challenges that we've been trying to solve, and one of the things that we've seen in our work is that the ability to measure data sets and around security actions and then map it to your HR hierarchy gives you the visibility to understand where your strengths and weaknesses are at an individual level, at a department level, and at an organizational level. And then map those behaviors over time.

Masha Sedova: 34:31

Why that's really important is because it's quite possible that there are parts of your human risks that are absolutely an acceptable level that you don't need to train people on. Your employees might already be really great at secure browsing for example, and you don't need to be including that as part of your trainings, because your employees are already practicing that. But it does help you highlight parts of your organization that need greater focus and intention on risks, and you get to see how it's compared not just to yourself over time, but also to other peers in your industry.

Masha Sedova: 35:08

Because it's hard to understand like, "Am I doing enough? And what does enough even look like?" So, trying to create some guard rails where executives can communicate we are here, this is what good enough looks like, and I know that given where my peers are, given where the spread of the landscape looks like and the places where we're not good enough. Back to what I was saying, cohort mapping. There are tools that are much more sophisticated than just more training that can actually help shape and drive our organization to improve those behaviors.

Bill Murphy: 35:43

I'm just going to ask a bit of a technical question. It's related to one of the slides. I think being well as human, we need a starting point. We need to know where our current state is. And so a lot of companies, CISOs, CIOs invested millions in phishing tools, DLP tools, password managers, [SEEM 00:36:03] systems, [CASBs 00:36:04], endpoint protection, on and on and on. How do you grab a hold of the current state so that you can then build upon that and show progress over time?

Masha Sedova: 36:18

We integrate with the logs of the technologies that you mentioned. So CASB solution, endpoint solutions, proxies for example. At a high level, all we're looking for is what was the event, what was the severity of the event, when did it happen, and to whom. Based on that we start creating map. We also integrate with HR systems, whether it be a Workday for example or even systems like an Octo or Salesforce that has some concept of HR data sets.

Masha Sedova: 36:49

Then we cross those two data streams to basically show you not just what event happened, but how does that map to other parts of your organization. Then we help correlate it across other types of behaviors. So we're looking to explore the concept of are certain behaviors predictive of another. So if someone who's late in training, are they notoriously bad at endpoint protection as well? Being able to have some predictive ability, just doing log file analysis on one particular technology like a CASB for example would leave out.

Masha Sedova: 37:31

Then secondly we can export part of our understanding of what the risk is for an individual to other technologies that might need to understand, "I'm dealing with a user. How security aware and security savvy is this user?" It might change the way that that technology interacts with an individual based on what we as a platform can tell them about.

Bill Murphy: 37:55

It's essentially looking at those various tools is looking at the event, the severity, and to whom it happened. From the myriad of logs that can be pulled from these systems, you're essentially narrowing the focus down to a few critical indicators. Then by looking at the HR systems, you can pull that data out into essentially an aggregation tool that then you can compare that against the different employees at scale so that you can create essentially a current state, and then you can manage that over time.

Masha Sedova: 38:26

You got it, yep.

Bill Murphy: 38:28

Okay, got it. That makes sense. Makes sense to me, which is different than this is just personal aggravation with KnowBe4. I'm sure you're aggravated too, but I am just a little bit tired of KnowBe4 is going to solve all my problems, that kind of a thing. In fact, I'm actively looking for a replacement for KnowBe4. Not because it's not a good tool, but people are coming to me going ... They're getting demos. They're not even doing demos anymore. They show you the quote, and then they want you to do a demo, and the people are confused by what they're seeing. It's really aggravating. I don't know if you want to comment to that, but I look at yours as being much more a comprehensive solution set versus that. Is that true?

Masha Sedova: 39:15

That's absolutely true. Back to the conversation of awareness versus behavior change, this is one of the biggest differences. When you have a content library, the only thing you're going to do is make people, ideally in a perfect world, aware. But I got to say rolling out just more training, every employee I talked to said, "Oh yeah, I get that, but I just mute it and I skip to the end and I guess this question." That's a reality that almost every organization faces.

Masha Sedova: 39:49

The thing that I would encourage everybody who's listening on this call is that when you do roll that out, yeah, it's easy just to hit send, but that's the voice and the face and the brand of the security team that all of your employees see. Your brand is connected to that mind-numbing training, regardless of the vendor. Unless you can meet your employees where they're at in a way that is actually engaging them and providing them meaningful feedback that actually helps them get better in the context of their work, it's not helping the relationship between the security team and your employees. That's a relationship that matters a lot, especially when you're asking your employees to report vulnerabilities and now that everyone's working from home, to be transparent and ask for help when they need it. And if you're not focusing on how you're building relationships with your employees and just sending it, it's a monologue and not a dialogue, which is truly what awareness training is most of the time. You're doing your organization a disservice.

Bill Murphy: 41:00

Maybe I listened to this in a different interview, but didn't you say 15%, it's a really low percentage, of learning is taken in I guess by these type of videos that are just pushed down? Isn't from a pure learning, that's one of the most effective ways to learn?

Masha Sedova: 41:18

Totally, yeah. This is part of the learning pyramid, and it talks about how we retain information. Things that are audiovisual at best have 15% retention no matter how good the content is. Our minds are not designed to retain that information, but if you go into a demo, it's 50%. And if it's active discussion, it's something like 70%. Practice by doing is 80, and then if you're teaching, you have 90% of the retention. So, if anyone has ever been forced to get up in front of somebody and teach a concept, that is the best way to retain that information.

Masha Sedova: 41:57

But yeah, if you have a video talking at you it doesn't matter how great it is, you're only going to remember 15% of it. Thinking through how other engagement methodologies is really helpful for helping our employees remember the information we're trying to give them.

Bill Murphy: 42:14

Well Masha, I really enjoyed this conversation. We're getting close to top of the hour, and I wanted to just as we wrap up, is there anything in particular that you are hoping that I'd ask or any final clarification that you're thinking, "You know what? I love to wrap up with any final thoughts."?

Masha Sedova: 42:33

I just wanted to do a quick comment around the crazy times we're living in right now and how leaders can start using this as a silver lining. Changing culture in your organization is hard. Changing behaviors is hard, because we get stuck in our habits and our routines as human beings. That's how we're wired to optimize living. And one of the best times in an organization to change your culture is in times of crises, because what we know to be normal and true is suspended, and we're willing to reevaluate those habits.

Masha Sedova: 43:10

Every organization in the world right now has a unique opportunity to think through how they want to be at the other end of this experience, and I would highly encourage the CIOs and CISOs of organizations to take a step back and say, "What is the security culture I want to have, and how can I start communicating it, motivating employees to do it, rewarding and incentivizing those types of behaviors?" Because you're going to find a lot less friction right now than you would in any other times.

Masha Sedova: 43:46

There's a really great book on this topic called the Power of Habit, and Charles Duhigg, who's done so much work in understanding habits, but he has a really great chapter specifically on changing organizational habits. Talks about the specific case study where great leaders leverage crises to change organizations. So, I would love to leave all the listeners of this with that call to action.

Bill Murphy: 44:13

That's going to be the title of this, what is the future culture you want to have. Thank you, Masha. This is great in fact. What a great way to end this. Thank you for leaning into how we can think from our strategic brains in the midst of crisis, and I think that's how leaders are reborn and how we all need to think about our own lives and our own families through this.

Bill Murphy: 44:39

Masha, thank you very much.

Masha Sedova: 44:41

Thank you, Bill. Really enjoyed this conversation.

Bill Murphy: 44:43

It's been a pleasure.

Masha Sedova: 44:45

Thank you.

Bill Murphy: 44:49

So there you have it. This wraps another episode of Bill Murphy's RedZone podcast. To get all the relevant show notes please go to our blog at www.redzonetech.net/podcast. Additionally, make sure you go to iTunes and leave your comments in iTunes about the show. This helps our show rankings enormously, and it helps support the show. Until next time, appreciate you very much for listening. Thank you.