The Weakest link

Presenter: Masha Sedova

Summary

Humans are often deemed the “weakest link” in security, and if organizations maintain that attitude with their employees then nothing will change. An encouraging and positive company culture can turn them into the most powerful weapon. Masha Sedova, co-founder of Elevate Security, takes listeners through the ways they can foster a more people-centered security approach for better results.

“In sophisticated attacks – let’s say like spear phishing, one that bypasses your entire tech stack – it takes one person to report it to your incident response team to totally throw a wrench into a sophisticated attack. So, while it does take one person to infect a network, it also only takes one person to flag something suspicious that can and does actually get past your tech stack. I do think there is a lot of hope in actually evolving our human element to be one of our layers of defense. It’s never going to be perfect, but it will be a layer.”
Transcript

Brian Contos:
Welcome to the Cybersecurity Effectiveness Podcast, sponsored by Verodin. The Verodin Security Instrumentation platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness. I'm your host, Brian Contos. We've got a very special guest today. Joining me is Masha Sedova. Welcome to the podcast, Masha.

Masha Sedova:
Hi, Brian. Great to be here.

Brian Contos:
Hey, Masha, before we begin, could you give our audience a little bit of background about you and your path and sort of what eventually led to your sort of current role?

Masha Sedova:
Yeah, absolutely. So, I knew that I wanted to get into CS, computers, ever since I was a little girl. My grandmother taught. My grandfather had a program. She was graduating class 1954 in Soviet Russia [as a] programmer. So, it's kind of been a thing my family has been doing for a long time. But I wanted to move away from just programming and I found the field of security when I still in college, fell in love with it. I love the idea of the fact that there're good guys versus bad guys and that the field is so dynamic. You can attack, you can defend, and then there's a whole human component, which I discovered a little bit later on in my career. So, I transitioned from more of a CS degree into the field of security in my last two years of school. Got a chance to work for the defense sector as a contractor and I was a cyber analyst.

Masha Sedova:
Again, speaking Russian, studying security, you can imagine there's a lot of interesting problem sets to solve in that space. Haven't quite figured out the Russian cyber threat is as we all know, but I take a crack at that. And somewhere along the way I realized it was always, there's always a human element associated with it, right? We can have the best offenses, but if your human element wasn't up to the task of defending against sophisticated attacks, you're not fighting with everything you have.

Masha Sedova:
So, I switched over to Salesforce, the private sector, in 2012, where I got to build and run a security engagement team. Really responsible for shifting the human element for internal employees, developers, and also getting Salesforce customers to adopt security features. I was obsessed with this question of “How do we get people to want to do security instead of have to?” Because coming from my days in the government, I knew that when we get people to have to do security, they just keep clicking on links and making mistakes...

Brian Contos:
Exactly.

Masha Sedova:
...and it's going to do nothing for us. So, I took that love of getting people to shift their behaviors and started my own company, elevate security, which focused on building a platform for security behavior change for companies of scale and getting people to really buy into shifting their mindset of security.

Brian Contos:
Oh, I love it. What an awesome background, and you mentioned some things in there that I think are really interesting. So, humans, what are they all about?
Masha Sedova:

Yeah.

Brian Contos:

So, is that the, you know, and I've heard some different perspectives on this. But somebody like you that's sort of tip of the spear for this, you know, are they the weakest link? Are they the first line of defense? Where do you fall on this?

Masha Sedova:

You know, that's a great question. And I feel like as an industry we've evolved our thinking on this significantly. I think if you were to ask the majority of CISOs, a decade ago, what they thought of the space, they will say obviously the weakest link, just look at any of your stats. And I think that, that is still the majority of the answers you'll get from something like 60% of the CISOs, but I'm seeing an evolution and a trend in our space. And this maps to my belief in what I've seen in my experience as well, is that if given enough resources, and also the correct type of resources, and we'll get into that in a little bit but what that looks like, your human element can actually be your first line of defense. And I know a lot of people are like, yeah, you say that, but I don't believe it because a lot of my incident response incidents are originated in human element.

Masha Sedova:

But what I've also seen is that in sophisticated attacks – let's say like spear phishing, one that bypasses your entire tech stack – it takes one person to report it to your incident response team to totally throw a wrench into a sophisticated attack. And if it takes a month for red team attack or yeah, planned or unplanned, to develop custom malware to get into your organization. One person reporting it to your security team is enough to significantly change the course of that attack to the detriment of the attackers. So, while it does take one person to infect a network, it also only takes one person to flag something suspicious that can and does actually get past your tech stack. So, I do think there is a lot of hope in actually evolving our human element to be one of our layers of defense. It's never going to be perfect, but it will be a layer.

Brian Contos:

Yeah. You know, and I like that perspective on it, because it's somewhat, it is contrarian to what a lot of people believe. I was just at Black Hat and you still see people walking around with shirts, like there's no patch for human stupidity, and all these types of things. Which makes me, you know, ask this question. So, I get it and I think that humans can be a valuable part, but is that predicated on really having a security culture as a core capability within your cyber defenses?

Masha Sedova:

Yeah, that's a great question. So, security culture, let me just define it for our listeners. Security culture and culture as a whole is the thing that happens when you're not looking. You have a security culture, whether or not you intended to or are fostering one. Your security culture could be people clicking on links and ignoring your security team's advice or your security culture is people proactively reporting and holding each other accountable. What happens is, how much do you own that security culture and how much do you invest in it? And how much do you support the positive behaviors associated with it. So, that people know, even if I'm not being watched here, this is the right thing to do. And the way you do that is by spending the time to explain to people why it's important. Treating them with respect, keep telling them that they're the dumbest thing in the equation. You're going to get that kind of output out. It's like, "Oh, if I'm the dumbest thing, I'll show you how much I need security in my life." Right?

Brian Contos:

Yeah.

Masha Sedova:

But if you spend time positively reinforcing the behaviors you want, like we do with our dogs and cats and our kids, like why not with our fellow employees? Like you'll start getting feedback around, your employees will start getting feedback around the things that they're being asked to do and it will become part of your defense as opposed to a liability.
Yeah. I like the way you phrase that because it’s, you know, there’s some differences. It seems like the way you approach this between a security culture, security behavior change and even security awareness, and in your approach to that. Do you think these are our three separate categories that have to be approached a little bit differently?

Masha Sedova:
Yeah. So I’ll start with security awareness, which is most of the topics, the label that we put on this work right now. But I’ve seen in my career and what I really like to say around this is awareness actually doesn’t matter. There are millions of people in the United States alone that know and are aware that smoking kills them and they still continue to smoke. It doesn't actually matter what you know, it matters what you do.

Brian Contos:
Sure.

Masha Sedova:
Same thing with passwords, right? How many of us know not to reuse passwords and to use unique and strong ones and yet how many of our employees actually still do that? Maybe security practitioners, too. So, awareness is knowledge. It's like, okay, so I need to do something. It's a part of it, but that you can't end there. Then you have your behavior change component of your behaviors. And behaviors are the measurable, observable things we do.

Masha Sedova:
How many reasonable passwords do we have? How many times did you tailgate? What is your malware infection rates? And those are the observable tip of the iceberg that is underlined by security culture, or that can be synonymous with security mindset. And culture, is the thing that drives us because it is what we believe in. It’s our values, it’s our beliefs, and it’s our assumptions. If I don’t think that security’s important or that my company values security, it will show up in my behaviors. You can force people to change their behaviors and they will, but they won't do it in a deep and meaningful way, in a sustainable way, unless you also focus on the culture. Which is the, why does this even matter? What is the value of this?

Brian Contos:
You know, I like that because I think the smoking analogy was great. We know it’s bad. Some people choose to ignore it and you know, more people choose to just embrace that, embrace smoking despite all the warning signs and things like that, and the same does apply to security. You're absolutely right. So it does make sense to have that change agent in there. Let's talk about what some cutting-edge companies are actually doing when it comes to having this, you know, people centered security approach.

Masha Sedova:
Yeah. So, I want to focus in on the security behavior part of what we’re talking about, because often when I go into an organization and say, ”Well, what do you want your organization to be?” They’ll say, ”Hey, I want people to not be as dumb and I want them to embed security to everything they do.” And that security mindset, that security culture and so it’s really hard to measure. It's really hard to shift. So the cutting edge people that I’ve seen in this industry have actually taken a step back and said, ”Well, when this culture exists, what will my organization look like? How can I quantify that we’re succeeding against this goal or not?” And so, they’ve prioritized the list of security behaviors that are most critical from a human element. Often top of mind becomes reducing phishing click through, which is not really a surprise, increasing reporting rate followed then by decreasing malware downloads, and then improve patching practices.

Masha Sedova:
Now your basic hygienes, but all hygiene components of security. But, you also have to realize that there’s a human component to every one of those things and we can influence and nudge people into better practices here. And so what they’re doing, associated with these behaviors, is tying it to existing data sets and saying, can I actually track where my organization is and can I improve this and see if I’m improving it. Because the thing that I’ve seen is that once you can associate a dataset with how your people are doing, you can figure out who is doing a great job and reward those, back to the point I was making earlier, about recognizing good behavior.
You can understand which people and which groups are not focusing on that and you can start doubling down your efforts there. And then you can also see when you’re done with the behavior, like is it at a threshold of risk that you can accept and then move on to the next thing that’s most important. So, it’s not this never-ending thing of communications and posters, you constantly have to keep putting up. You might actually be at a good place of malware downloads. So, you don’t actually have to focus your mental energy as a culture on this specific topic.

Brian Contos:
You know and that brings up an interesting question, when we talk about security, we’re always talking about trying to measure it and ROI calculations, return investment or seeing how we get value. How do you really do that when it comes to security awareness and security culture?

Masha Sedova:
Yeah. So current best practices are, unfortunately, has two ROI metrics associated with it. Which is why I actually think the industry hasn’t gotten as far, this part of their industry hasn’t gotten as far. And those two metrics are how many people have completed a training and what is my phishing click through rate, my mock phishing click through rate, not my real one. And that's all the metrics that we have.

Masha Sedova:
And the training thing is so broken because it's oriented around compliance. It doesn't actually give me a risk lens. And there's actually a lot of pain points in the phishing click through ones as well, because you have to really make sure that you are tracking that on with a like for like type of phishing test versus arbitrary difficulty. So if we take a step back, the best way to measure ROI for a security team across any department, the human element or otherwise, is a risk centric metric.

Masha Sedova:
Am I reducing risk for my organization? And the way that you tie that is to the human programs you have, is understanding where are your greatest user generated incidents. So those are some of the top four behaviors that I mentioned. And then trying to understand where your current posture is by getting the data sets around it and then reducing those behaviors over time. But ROI should be measured by the decrease in events or increase in desirable events of what your humans are doing. And if you can't measure what you're doing, you can't figure out an ROI on your program. That's the tangible ROI.

Masha Sedova:
There is a second component of it that's so much more intangible and that is your internal brand as a security leader or as a security team. When you start communicating in a way that isn't just punishment but rewarding people for good behaviors and also giving people clear and understanding deliverables, it actually builds a level of rapport or even potentially trust between the security team and the rest of the organization. Because you don't always just get to be the department of no, you actually set clear milestones and goals for the rest of your org, which really helps getting people on your team.

Brian Contos:
Yeah and I liked that because you know, you start off by talking about some of these quantitative measurable, fact-based, proof-based metrics, which I think are, you know, everybody wants to try to measure things so they can improve. But there is a qualitative aspect to this where it's going to be hard to put something on a chart to say it's better than it was before, but you do have this kind of visceral reaction to a team that's actually helping to enable, instead of to your point, the department of no and it certainly makes it easier to embrace these changes that you're talking about.

Masha Sedova:
Mm-hmm.

Brian Contos:
I'm wondering when it comes to security behavior, given that all you've seen and all you've done in your career, is there one particular thing or a group of things that you just wish employees would change?
Yeah, that's a good question. I think that the metric that I wish more security teams would drive focus on is driving reporting rates from your employees to your security teams about things that they see as unusual. Because what starts happening is you're asking, you're delegating your vigilance of security to outside of your organization and you're creating that communication and exchange. Not only does it help sort of from a security culture perspective, but it also is the thing that's going to start tuning your employees to be a layer of defense that will add on to all the technology that you've invested in. And if you think about it, your technology will fail sometimes, humans will fail sometimes, your processes will fail sometimes, but ideally if all three are working, one of them will catch what the other one hasn't. And if we don't train our employees to report when things seem unusual, we're missing a full layer of defense around what our employees can absolutely be doing to help us in detecting anomalies and course correcting to make us a more secure organization. So that's my one wishlist behavior for every org.

Brian Contos:
Yeah. That's right in cyber we've been talking about for years. You know, you prevent where you can, when you can't you try to detect, so therefore you can respond effectively and efficiently and it's, you know, without one piece hopefully one of the other pieces kicks in. And this is the first time I've actually heard anybody talk about layering that human element to augment that. So that's very, very interesting. So, Masha, as we wrap up here, there's a question we'd like to ask everybody on the show and that's who's your favorite superhero or super villain and why?

Masha Sedova:
Hands down, my favorite superhero/villain, it depends on your perspective, is Mystique from X-Men. Not only do I think she has the most bad-ass superpower and she can become anybody, I really like the way that she holds that superpower. She can be so deadly, but she doesn't run around and like make a ruckus blowing things up. She's just like precise and very, very thoughtful in her actions, and at the same time incredibly impactful. I love that she just says the right thing and the right time to cause enough chaos or resolve situations. Mostly chaos, I imagine.

Brian Contos:
No, I love it. If I was a betting man, I would have said Black Widow, just given your background and hers, but you threw Mystique in there but a great one.

Masha Sedova:
Yeah. Uh-huh.

Brian Contos:
All right. Well thanks so much, Masha, and thanks to all our listeners for joining and be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.